OŚWIADCZENIE O PRAKTYKACH CERTYFIKACJI

ELECTRONIC IDENTIFICATION, S.L.

KONTROLA I ŚLEDZENIE DOKUMENTU

Wersja	Data	Wykonanie	Sprawdzenie	Zatwierdzenie
1.1.	2020-02-27	Cristina Romera Soto (Obszar prawny)	Carlos Sáez Quintero	Iván Nabalón Barrientos CEO
1.1.	29.05.2020	Cristina Romera (Obszar prawny) Albert Borrás	Iván Nabalón Barrientos (CEO)	Iván Nabalón Barrientos CEO
1.2.	25.05.2021	Cristina Romera Soto (Obszar prawny)	Iván Nabalón Barrientos (CEO)	Iván Nabalón Barrientos CEO
1.3.	15.10.2021	Francisco J. Ferrándiz (Obszar prawny)	Iván Nabalón Barrientos (CEO)	Iván Nabalón Barrientos (CEO)
1.4.	21.10.2021	Francisco J. Ferrándiz (Obszar prawny)	Iván Nabalón Barrientos (CEO)	Iván Nabalón Barrientos (CEO)
1.5.	22.10.2021	Francisco J. Ferrándiz (Obszar prawny)	Iván Nabalón Barrientos (CEO)	Iván Nabalón Barrientos (CEO)
1.6.	03.12.2021	Cristina Romera Soto (Obszar prawny)	Iván Nabalón Barrientos (CEO)	Iván Nabalón Barrientos (CEO)

Spis treści

1. Wstęp

1.1. Prezentacja

Niniejszy dokument zawiera odniesienia dla przygotowania Kodeksu Postępowania Certyfikacyjnego, opisujące każdą z sekcji, które należy wykonać, zgodnie ze standardem RFC 3647.

ELECTRONIC IDENTIFICATION, SL, chroniona słownym znakiem wspólnotowym (MC), jest spółką zarejestrowaną w Rejestrze Handlowym w Madrycie w dniu 13 marca 2013 r. pod numerem NIF B86681533 i danymi rejestracyjnymi: Tom: 30920, Książka: 0, Kartka: 146, Sekcja: 8, Kartka: M5506508, z datą 3 kwietnia 2013 roku.

1.2. Nazwa dokumentu i identyfikacja

Ten dokument jest OŚWIADCZENIEM O PRAKTYKACH CERTYFIKACJI

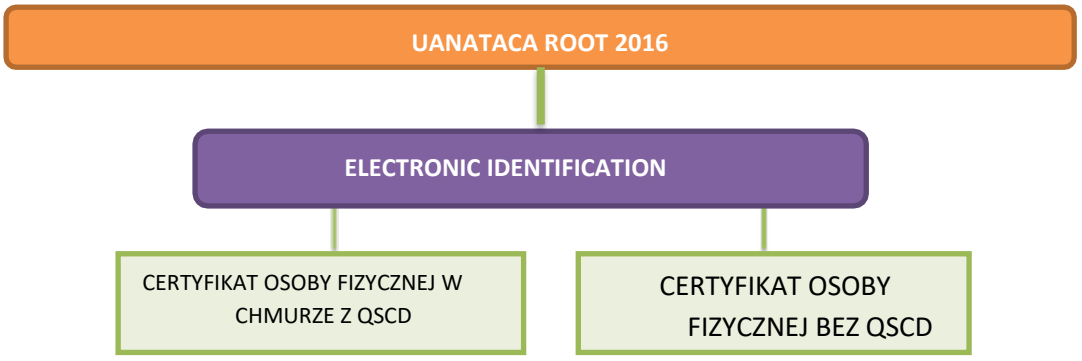
1.3. Uczestnicy w usługach certyfikacji

1.3.1.1. Dostawca usług certyfikacji

Dostawcą usług certyfikacji elektronicznej jest osoba fizyczna lub prawna, która wydaje i zarządza certyfikatami dla podmiotów końcowych za pomocą Urzędu Certyfikacji lub świadczy inne usługi związane z podpisami elektronicznymi.

ELECTRONIC ID jest dostawcą elektronicznych usług zaufania, który działa zgodnie z przepisami Rozporządzenia PARLAMENTU EUROPEJSKIEGO I RADY (UE) 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania dla transakcji elektronicznych w zakresie rynku i przez który dyrektywa 1999/93/WE zostaje uchylona, a także normy techniczne ETSI mające zastosowanie do wydawania i zarządzania kwalifikowanymi certyfikatami, głównie EN 319 411-1 i EN 319 411-2, w celu ułatwienia zgodności z wymogami międzynarodowymi uznania jej usług.

W celu świadczenia usług certyfikacyjnych EID ustanowiła hierarchię jednostek certyfikujących:



1.3.1.2. UANATACA ROOT 2016

Jest to główny urząd certyfikacji w hierarchii, wydający certyfikaty innym jednostkom certyfikującym i którego certyfikat klucza publicznego został podpisany przez samego siebie.

Dane identyfikacyjne:

- CN: UANATACA ROOT 2016
- Cyfrowy odcisk palca: 2e69a72bcbf9df1f560be51388d636703d5927ed
- Ważny od: 2016-03-11
- Ważny do: 11 marca 2041
- Długość klucza RSA: 4.096 bits
- URL: https://web.uanataca.com/common/project/pdf/autoridad-certificacion/01_raiz-ca-2016.cer

```
-----BEGIN CERTIFICATE-----
MIIHAzCCBOugAwIBAgIITWOS6Y7X5ZQwDQYJKoZIhvcNAQELBQAwgbkxCzAJBgNV
BAYTAkVTMUQwQgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3Mg
YXQgd3d3LnVhbmF0YWNhLmNvbS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0Eg
Uy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNBMRswGQYDVQQDDBJVQU5BVEFDQSBS
T09UIDIwMTYxGDAWBgNVBGEMD1ZBVEVTLUE2NjcyMTQ5OTAeFw0xNjAzMTEwOTEz
NTNaFw00MTAzMTEwOTEzNTNaMIG5MQswCQYDVQQGEwJFUzFEMEIGA1UEBww7QmFy
Y2Vsb25hIChzZWUgY3VycmVudCBhZGRyZXNzIGF0IHd3dy51YW5hdGFjYS5jb20v
YWRkcmVzcykxFjAUBgNVBAoMDVVBTkFUQUNBIFMuQS4xFTATBgNVBAsMDFRTUC1V
QU5BVEFDQTEbMBkGA1UEAwwSVUFOQVRBQ0EgUk9PVCAyMDE2MRgwFgYDVQRhDA9W
QVRFUy1BNjY3MjE0OTkwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
d5rtQey704cMzz7A1vuB4HLs0Y8YlH7BXKFAuxwzst1GOl7TzZzOeDEjGZMSjI00
JRUdmZ/lmG927tES5dDlrfDrNvKu3mof9j6Wjch4HmNqT6I30TXnhBNbtKEYHWxC
cIvQ0OKaFUUBEt+NzS6smyDAzbwyFUPSPid8JoGaGUMy7hhah38cLN408ffigCFT
ehZIsRvDnsU1WU34vcAYLLmgjsvBNmq2V+Ts8+vtrLcRbpQ8usMbwJSO1aoi71Lu
ISeBGJjqaszMPOty923PGHemImxHl5mHT13k5ha98EK4ZXMFfjxSVrypvpHgjThU
V3s4ZeaSpSbWkFxl6Tl++OTciMLOp66jwZV3I4DqeRmNXJkiRebs5u8bDDZxxeSP
RusoFI1cLm9cqCNy51hd2LNv8QECUNQ/RPon0sh+BSoSedppYXq6TFqpabE/FTnt
JBU7CMJV3EFJ/jSvXf6qj7JjInUQXajSxDdt0WrmDW8aQCRKCZ0Ml/Iwb8yk83/y
ZDt6E+Ez63V/x7sA2ZygG61zf4wOT95FNA4Z1atfOEcp/2uc5HXKrUTXTMDJJZfD
WMo30Ae1Rei94TRd/9XRqPdEk0B/VL5/991SlEX6Ol0NwKRPm6HNNZoWbdnmLEc+
CGnX1yj01R51Y4UTOalJ/W7oiNxmpZQAdAc9NN/gkwIDAQABo4IBCzCCAQcwHQYD
VR0OBBYEFFUs8byhXrnuoC+IVxBb/Jb3kZosMA8GA1UdEwEB/wQFMAMBAf8wgaYG
A1UdIASBnjCBmzCBmAYEVR0gADCBjzAzBggrBgEFBQcCARYnaHR0cDovL3d3dy51
YW5hdGFjYS5jb20vcHVibGljL3BraS9kcGMvMFgGCCsGAQUFBwICMEwMSkNlcnRp
ZmljYWRvIHJhw616IGRlIFVBTkFUQUNBLiBWZXIgaHR0cDovL3d3dy51YW5hdGFj
YS5jb20vcHVibGljL3BraS9kcGMvMA4GA1UdDwEB/wQEAwIBBjAcBgNVHREEFTAT
gRFpbmZvQHVhbmF0YWNhLmNvbTANBgkqhkiG9w0BAQsFAAOCAgEATAyOSKmK/yj6
JFb/RaHMmor8knkwQWVi3lFASKyfLQc6FfHoVjEgihu6HekIlMS7WBzetQVomaTR
TDu6eJeyo/+7CB+VGGHOYYjSdc8F8WI1HFN3f6ztKuM6zlVz3Xyj9BHhg1H4gqNL
Yxe99kq14xQEOR/fm0p7rVgVeeHhG8m1S5UGyyJ1ukeiB0d0PqwVWlG1np+i/nhf
nrxGSTnbRJyHzx6tuaLuQyHQU+Dg0TS8k65a8URioVkQ0CWb7yIyJ5bEBmPR2yqX
Owt6nYR8/3blrU99+wp67pmQttSggX3sB2a9WfY94Y5uIPB7JisOUBmqH23RjakE
c+UMLMjnvJQ82+1M7oGebnaVd1RVK+okemQ5zx57BzkzSl/i4G+Zxya8oQb2cIqF
HnvyCVXDOd4/CWNBLZQCTyGRUKOocvu1kKXgmVY6hTQGhM8Tr5yg/XT21gaAv3/7
th5ib2iGgq8Q8E3AW3ND+8N/qMjZ2aIkBKQYUFmLWiZt6n6ni73E2LQQEs+0uh9+
1xTPcI7AfDv+p0m6HDP0pq0t7BX0DQbh5QwPpiHBkB8atzE5gmQxnkt4/g0S2av5
Lc+U7ufZ5/ao7tLL1qkTX2r87jN7T8+lZOSHBbQan2QosyBfZWXgxaFYTspoy5tP
n4RMcCgXqHSYlArUKaQ8OWmT42AKLdY=
-----END CERTIFICATE-----
```

1.3.1.3. EID CA1

Jest to główny urząd certyfikacji w hierarchii, wydający certyfikaty innym jednostkom certyfikującym i którego certyfikat klucza publicznego został podpisany przez samego UANATACA ROOT 2016.

Dane identyfikacyjne:

- CN: EID CA1
- Cyfrowy odcisk palca: 2e69a72bcbf9df1f560be51388d636703d5927ed
- Ważny od: Wtorek, 25.02.2020
- Ważny do: Środa, 24.02.2033
- Długość klucza RSA: 4.096 bits
- URL:https://www.electronicid.eu/assets/documents/ELECTRONICIDENTIFICATIONCA1. pem.cer

```
-----BEGIN CERTIFICATE-----
MIIIdTCCBl2gAwIBAgIINsAgN1d7Z1EwDQYJKoZIhvcNAQELBQAwgbkxCzAJBgNV
BAYTAkVTMUQwQgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3Mg
YXQgd3d3LnVhbmF0YWNhLmNvbS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0Eg
Uy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNBMRswGQYDVQQDDBJVQU5BVEFDQSBS
T09UIDIwMTYxGDAWBgNVBGEMD1ZBVEVTLUE2NjcyMTQ5OTAeFw0yMDAyMjUxMDU3
MTNaFw0zMzAyMjQxMDU3MTNaMIGbMQswCQYDVQQGEwJFUzEPMA0GA1UEBwwGTUFE
UklEMScwJQYDVQQKDB5FbGVjdHJvbmljIElkZW50aWZpY2F0aW9uIFMuTC4xEDAO
BgNVBAsMB1BTQy1FSUQxJjAkBgNVBAMMHUVMRUNUUk9OSUMgSURFTlRJRklDQVRJ
T04gQ0ExMRgwFgYDVQRhDA9WQVRFUy1CODY2ODE1MzMwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQDAFOTSwnEBJSAM6h9FT5ETiVHAtI1K885qGC6Bd+5i
UMhUmHUek5m1PZxJzUsMUNndPBfaRIi2os4upOnwrwNsk0bOfdTKh6qwmN5Uqstb
L9QH2W3eLYeUZHH11dY/be3PZSUICrMZZRUT/YP5GBhhJR+uy69AYJ8VzeLwjMtl
guse840QBRALuPRP7Q4U2P//hfFvw2vlZAEpnAFeO4pK6Ey9dzXciZpPteL/9CYf
1Cl48fNpFs85Pjsl/2xKycrRIYc0dCTe6yCTlzFPbZX5xsKicMzvFdsN//6BFckb
/1f8hW7ywZkgBHUfuvNkLrL7LfDdvYdGM8vzfS5Ozz7j+nXFs1MYc0g4iIumynhp
tmpkR1n/+JDMNf3uTFWlXUZO9dy4cfr7zqLm+Y+a+6ARud8K8aKRCHUFqOEMWKJB
4T7C1a1+/omPvXeAHjB8nt1Eqw4tACQQhbB3AHbdd5bnwp4mxu/o97kvfI0TCE5c
+IqacLZWW8SXDmRHv2hQTkCA1Gte5qJLnC/M0aWbyd0XFkYj9Xjzoa4k0oYSRI+0
wbKrhTlYQu8t14dLvOxujfRlOx1ZZfQwVEqPvIJjN8t5K97POI2kyaoOcFG5iwAo
06bvLfxEgq7kDU05OZ0UxZut5Q7SUB9f9lkA9bFkeg+9RQtBSNUdj7BCosvJmaOQ
0wIDAQABo4ICmzCCApcwfgYIKwYBBQUHAQEEcjBwMDYGCCsGAQUFBzABhipodHRw
Oi8vb2NzcDEudWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvb2NzcC8wNgYIKwYBBQUH
MAGGKmh0dHA6Ly9vY3NwMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9vY3NwLzAd
BgNVHQ4EFgQUhRVkzZsHSJ335ppEB5x5Coyhlj8wEgYDVR0TAQH/BAgwBgEB/wIB
ADAfBgNVHSMEGDAWgBRVLPG8oV657qAviFcQW/yW95GaLDAcBgNVHRIEFTATgRFp
bmZvQHVhbmF0YWNhLmNvbTCB4wYDVR0gBIHbMIHYMIHVBgRVHSAAMIHMME0GCCsG
AQUFBwIBFkFodHRwczovL3d3dy5lbGVjdHJvbmljaWQuZXUvY2VydGlmaWNhdGlv
bi1wcmFjdGljZS1zdGF0ZW1lbnQtY3BkLzB7BggrBgEFBQcCAjBvDG1DZXJ0aWZp
Y2FkbyBkZSBsYSBBdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2nDs24gU3Vib3JkaW5h
ZGEgZGUgRWxlY3Ryb25pYyBJRGVudGlmaWNhdGlvbi4gLSB3d3cuZWxlY3Ryb25p
Y2lkLmV1MIGLBgNVHR8EgYMwgYAwPqA8oDqGOGh0dHA6Ly9jcmwxLnVhbmF0YWNh
LmNvbS9wdWJsaWMvcGtpL2NybC9hcmxfdWFuYXRhY2EuY3JsMD6gPKA6hjhodHRw
Oi8vY3JsMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9jcmwvYXJsX3VhbmF0YWNh
LmNybDAOBgNVHQ8BAf8EBAMCAQYwHwYDVR0RBBgwFoEUaW5mb0BlbGVjdHJvbmlj
aWQuZXUwDQYJKoZIhvcNAQELBQADggIBABd3oBLIIp7Saspm9DWVMudT79NCJ02h
00t8P1PZR0zz3KAkdrO4G1hg92vKqzhjgJsHMYt2zV8XYQ487T2S/pKbIMTTDFHR
wSNyU5S4z8p4gufCF8kkrZlRim0SKBtiaYnKLqmtiyiLjnPvegwpq3gVcg8afKI5
qxnShchNH+lveNx/QC7MePku0FAZY9naFEPmcdSs3mGiVHZbuv5eWsqm4/BMx+4X
```

PBmHO8Vjj2HzUdfCcavkXkocDA8+7WB+aQHZ3gHZQvC0pFKSwO6YSdo8d/IfICzU
J7yADUkVvDW4DMox6GwnXc8b9WQkjWHPXSHLMs93kzLtE3Lws9C//I1lMbf4o7U4
wkt55M3nYO2mt7AEwS9oKSDr3hQsN6IA/IMwoYj4oML9U6ytcYTNUQINRWShyLdf
WMwtOZmhlQXbbYqlXHhwVqL1hjlQ6bPOARKOo186ol5cP0LEV4ehDDVQoHZFgRje
MPD/UEQp83v9Q4swHZjzTlsBhlRhZH5g+TWXTYBPOs94quaJRI9QVlVk7ICEsQA6
11F1XG4tkX7CuvuOdPjv1VBrJPM4oREsU1YXxNzew3+NH1IJ4SS/RpwiwctUpepR
vRyrQlKf4bHqMTXh04CsE19fE8RLjxy7VnCDTbrYo7TCAoQQMbQwK9nEOIOOeTs2
d3QXqGqKXRth
-----END CERTIFICATE-----

1.3.2. Organy rejestracyjne

Punktem Rejestracji może być osoba fizyczna lub prawna działająca zgodnie z niniejszym Kodeksem Postępowania Certyfikacyjnego oraz w stosownych przypadkach, na podstawie umowy podpisanej z określonym CA, pełniąca funkcje zarządzania aplikacjami, identyfikowania i rejestrowania wnioskodawców certyfikatu. oraz te, które są dostępne w określonych Politykach Certyfikacji. RA są organami delegowanymi CA, chociaż CA jest ostatecznie odpowiedzialny za usługę.

Punkt Rejestracji EID to podmiot odpowiedzialny za:

- Przetwarzaj żądania certyfikatów
- Zidentyfikuj wnioskodawcę i sprawdź, czy spełnia on wymagania niezbędne do ubiegania się o certyfikaty.
- Potwierdź sytuację osobistą osoby, która będzie występować jako sygnatariusz zaświadczenia.
- Zarządzaj generowaniem kluczy i wydawaniem certyfikatu.
- Dostarcz certyfikat subskrybentowi lub środki do jego wygenerowania.
- Opieka nad dokumentacją związaną z identyfikacją i rejestracją podpisujacych i/lub użytkowników oraz zarządzaniem cyklem życia certyfikatów.

Może działać jako EID RA:

- Każdy podmiot upoważniony przez EID
- EID bezpośrednio

EID sformalizuje umownie relacje między sobą a każdym z podmiotów pełniących funkcję Punktu Rejestracji EID

Podmiot pełniący funkcję Punktu Rejestracji ŚIE może upoważnić jedną lub kilka osób jako Operator RA do obsługi systemu wydawania certyfikatów ŚIE w imieniu Punktu Rejestracji.

Urząd Rejestracyjny może delegować funkcję identyfikacji użytkowników lub podpisujących, pod warunkiem wcześniejszej umowy współpracy w którym zostanie zaakceptowana delegacja tych funkcji. EID musi wyraźnie upoważnić wspomnianą umowę o współpracy.

Również Urząd rejestracyjny objęty tym Oświadczeniem Praktyk Certyfikacji, oddziały wyznaczone do tej funkcji przez użytkowników certyfikatów jako departament personelu, gdyż posiadają autentyczne rejestry dotyczące relacji podpisujących z użytkownikami.

1.3.3. Użytkownicy

Użytkownicy usługi certyfikacji to:

- Firmy, podmioty, korporacje i organizacje, które nabywają EID (bezpośrednio lub za pośrednictwem strony trzeciej) do użytku w swoim korporacyjnym środowisku biznesowym i są identyfikowani certyfikatami.
- Osoby fizyczne, które nabywają certyfikaty dla samych siebie, są identyfikowane certyfikatami.

Użytkownicy usługi certyfikacji uzyskuje licencję na korzystanie z certyfikatu do własnego użytku - certyfikatu pieczęci elektronicznej - lub w celu ułatwienia poświadczenia tożsamości konkretnej osoby należycie upoważnionej do różnych czynności w sferze organizacyjnej użytkownika - certyfikaty podpisu elektronicznego. W ostatnim przytoczonym przykładzie osoba ta jest wskazana na certyfikacie.

Użytkownik elektronicznej usługi zaufania jest zatem klientem dostawcy usług certyfikacyjnych, zgodnie z prawem prywatnym, ma prawa i obowiązki określone przez dostawcę usług certyfikacyjnych, które są dodatkowe i zrozumiałe bez uszczerbku dla praw i obowiązków dla podpisującego, jako upoważnionych i uregulowanych w europejskich normach technicznych mających zastosowanie do wydawania kwalifikowanych certyfikatów elektronicznych, w szczególności ETSI EN 319 411, rozdziały 5.4.2 i 6.3.4.).

1.3.4. Zaufanie obustronne

W niniejszym CPS przez Stronę Użytkownika lub użytkownika rozumie się osobę, która otrzymuje transakcję elektroniczną dokonaną za pomocą certyfikatu wydanego przez którykolwiek z Urzędów EID i która dobrowolnie ufa wydanemu przez niego Certyfikatowi.

1.3.5. Inni uczestnicy

Dostawca usług Infrastruktury klucza publicznego

EID i UANATACA, S.A. podpisali umowę na świadczenie usług technologicznych, w ramach której UANATACA dostarczy infrastrukturę klucza publicznego (PKI) wspierającą obsługę zaufania EID.

W taki sposób UANATACA udostępnia EID niezbędny personel techniczny do prawidłowego wykonywania wiarygodnych funkcji Dostawcy Usług Zaufania.

Oznacza to że, UANATACA jest skonfigurowana jako dostawca usług infrastrukturalnych dla usług certyfikacyjnych, świadczy swoje usługi technologiczne na rzecz EID, aby mogła realizować usługi nieodłącznie związane z dostawcą usług zaufania, gwarantując przez cały czas ciągłość usług w warunkach i w należnych warunkach przepisowych.

Równomiernie informuje się, że UANATACA jest akredytowanym Dostawcą Usług Zaufania zgodnie z przepisami Rozporządzenia Europejskiego nr 910/2014 Parlamentu Europejskiego i Rady z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania dla transakcji. na rynku wewnętrznym i uchylające dyrektywę 1999/93/WE (rozporządzenie eIDAS).

UANATACA PKI przechodzi coroczne audyty w celu oceny zgodności kwalifikowanych dostawców usług zaufania zgodnie z obowiązującymi przepisami norm ISO/IEC 17065:2012, ETSI EN 319 403 V2.2.2., ETSI EN 319 421 v1.1.1, ETSI EN 319 401
v2.1.1, ETSI EN 319 411-2 v 2.1.1, ETSI EN 319 411-1 v 1.1.1.

1.4. Używanie certyfikatów

1.4.1. Dozwolone zastosowania certyfikatów

Certyfikat kwalifikowany Osoby Fizycznej w CHMURZE bez QSCD

Ten certyfikat posiada OID 1.3.6.1.4.1.55193.1.1.1. Jest to certyfikat kwalifikowany, który jest wystawiany do zaawansowanego podpisu elektronicznego i uwierzytelniania, zgodnie z polityką certyfikacji QCP-n z OID 0.4.0.194112.1.0. Certyfikaty dla osób fizycznych w CHMURZE są certyfikatami kwalifikowanymi zgodnie z postanowieniami art. 24 i 28 Rozporządzenia (UE) 910/2014.

Gwarantują tożsamość użytkownika i osoby wskazanej w certyfikacie oraz umożliwiają generowanie „zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie elektronicznym".

Certyfikaty mogą być używane w aplikacjach takich jak:

a) Uwierzytelnianie w systemach kontroli dostępu.

b) Bezpieczny podpis poczty elektronicznej.

c) Inne aplikacje wymagające podpis elektroniczny, zgodne z ustaleniami obu stron lub z obowiązującymi w danym przypadku normami prawnymi.

Informacje o zastosowaniach w profilu certyfikatu wskazują następująco:

Pole „key usage" jest aktywne, w związku z tym pozwala realizować następujące funkcje:

a. Podpis cyfrowy (Podpis cyfrowy, do wykonywania funkcji uwierzytelniania)

b. Zobowiązanie do treści (Content commitment, do wykonania funkcji podpisu elektronicznego)

c. Key Encipherment

Certyfikat kwalifikowany Osoby Fizycznej w CHMURZE z QSCD

Ten certyfikat posiada OID 1.3.6.1.4.1.55193.1.1.2. Jest to certyfikat kwalifikowany, który jest wystawiany do kwalifikowanego podpisu elektronicznego i uwierzytelniania, zgodnie z polityką certyfikacji QCP-n-qscd z OID 0.4.0.194112.1.2. Tenże certyfikat wydany w scentralizowanym QSCD jest certyfikatem kwalifikowanym zgodnie z postanowieniami art. 28 Rozporządzenia (UE) 910/2014.

Współpracuje z uprawnionymi urządzeniami do składania podpisów (QSCD), zgodnie z artykułami 29 i 51 Rozporządzenia (UE) 910/2014 oraz jest zgodny z postanowieniami przepisów technicznych Europejskiego Instytutu Norm Telekomunikacyjnych, identyfikowanych odnośnikiem ETSI EN 319 411 -2.

Gwarantuje tożsamość podpisującego i jego relacje z użytkownikiem elektronicznej usługi zaufania, umożliwiając generowanie „kwalifikowanego podpisu elektronicznego"; czyli podpis zaawansowany, który jest oparty na kwalifikowanym certyfikacie i został użyty przy użyciu kwalifikowanego urządzenia, a więc ma równowartość podpisu pisemnym ze skutkiem prawnym, bez konieczności spełnienia jakichkolwiek innych dodatkowych wymagań.

Mogą być również wykorzystywane w aplikacjach, które nie wymagają podpisu elektronicznego równoważnego podpisowi pisemnemu, takich jak aplikacje wymienione poniżej:

a) Bezpieczny podpis poczty elektronicznej.

b) Inne aplikacje z podpisem elektronicznym.

Informacje o zastosowaniach w profilu certyfikatu wskazują następująco:

Pole „key usage" jest aktywne, w związku z tym pozwala realizować następujące funkcje:

a. Podpis cyfrowy (Podpis cyfrowy, do wykonywania funkcji uwierzytelniania)

b. Zobowiązanie do treści (Content commitment, do wykonania funkcji podpisu elektronicznego)

c. Szyfrowanie klucza

1.4.2. Ograniczenia i zakazy używania certyfikatów

Certyfikaty są wykorzystywane do wybranych funkcji i ustalonego celu, bez możliwości wykorzystania ich w innych funkcjach i do innych celów.

Również oznacza to, że certyfikaty muszą być używane wyłącznie zgodnie z obowiązującymi przepisami, zwłaszcza z uwzględnieniem istniejących w danym momencie ograniczeń importowych i eksportowych.

Certyfikatów nie można używać do podpisywania certyfikatów kluczy publicznych ani podpisywania list odwołania certyfikatów (CRL).

Certyfikaty nie zostały zaprojektowane, nie mogą być przydzielone, a ich użycie lub odsprzedaż nie jest dozwolona jako wyposażenie kontrolne w sytuacjach niebezpiecznych lub do zastosowań wymagających działań bezpiecznych w przypadku awarii, takich jak eksploatacja obiektów jądrowych, systemów nawigacyjnych lub łączności lotniczej, lub systemy kontroli broni, których awaria może bezpośrednio zagrażać życiu lub szkód środowisku w poważny sposób.

Wykorzystanie certyfikatów cyfrowych do czynności sprzecznych z niniejszym Kodeksem Postępowania Certyfikacyjnego, dokumentami prawnymi wiążącymi każdy certyfikat lub umowami z podmiotami rejestrującymi lub ich podpisującymi lub użytkownikami jest uważane za niewłaściwe wykorzystanie do celów prawnych. w oparciu o obowiązujące prawo, jakiejkolwiek odpowiedzialności za niewłaściwe użycie certyfikatów przez podpisującego lub jakąkolwiek stronę trzecią.

EID nie ma dostępu do danych, na których można zastosować certyfikat. W związku z tym i w konsekwencji tej technicznej niemożności dostępu do treści wiadomości, EID nie może dokonać żadnej oceny tej treści, tym samym pozostawiając na użytkowniku, osobie podpisującej lub osobie z odpowiedzialną za opiekę, jakąkolwiek odpowiedzialność wynikającą z treści związanych z wykorzystaniem certyfikatu.

Podobnie użytkownik, podpisujący lub osoba odpowiedzialna za opiekę będą ponosić jakąkolwiek odpowiedzialność, która może wyniknąć z ich wykorzystania poza ograniczeniami i warunkami użytkowania zawartymi w niniejszym Kodeksie Postępowania Certyfikacyjnego, wiążących dokumentach prawnych z każdym certyfikatem, lub umowy z podmiotami rejestrującymi lub ich użytkownikami, a także wszelkie inne niewłaściwe ich użycie wynikające z tej sekcji lub które mogą być interpretowane jako takie na podstawie obowiązujących przepisów.

1.5. Administracja publiczna

1.5.1. Organizacja zarządzająca dokumentem

ELECTRONIC IDENTIFICATION, S.L.: B-86681533
Avenida Ciudad de Barcelona, 81. 4ª Planta
28007 Madrid (Hiszpania)

1.5.2. Dane kontaktowe

ELECTRONIC IDENTIFICATION, S.L.: B-86681533
Avenida Ciudad de Barcelona, 81. 4ª Planta
28007 Madrid (Hiszpania)

1.5.3. Procedury zarządzania dokumentami

System dokumentów i organizacji EID gwarantuje, poprzez istnienie i stosowanie odpowiednich procedur, prawidłowe utrzymanie tego dokumentu i specyfikacji związanych z nim usług.

1.5.4. Łuk OID i EID

IANA, w swoim rejestrze PEN (Private Eterprise Numbers) przypisała identyfikatorowi elektronicznemu OID: 55193. Więc twój łuk OID zaczyna się od 1.3.6.1.4.1.55193

1.5.5. Główne OIDs polityki certyfikatów

W niniejszym CPS rozważa się następujące znaczenia OID:

CERTYFIKAT	Identyfikator OID
Certyfikat Kwalifikowany Oprogramowanie Osoby Fizycznej zarządzane przez Użytkownika	1.3.6.1.4.1.55193.1.0.1
Certyfikat Kwalifikowanej Osoby Fizycznej z QSCD zarządzany przez Użytkownika	1.3.6.1.4.1.55193.1.0.2
Certyfikat Kwalifikowany Osoba Fizyczna w CHMURZE bez QSCD	1.3.6.1.4.1.55193.1.1.1
Certyfikat Kwalifikowany Osoba Fizyczna w CHMURZE z QSCD	1.3.6.1.4.1.55193.1.1.2

2. Publikacja informacji i depozyt świadectw

2.1. Repozytoria

EID posiada Repozytorium Certyfikatów, gdzie publikowane są informacje związane z usługami certyfikacyjnymi.

Wspomniana usługa jest dostępna 24 godziny na dobę, 7 dni w tygodniu, a w przypadku awarii systemu poza kontrolą EID, ten zrobi wszytko co możliwe, żeby usługa jest ponownie dostępna w okresie określonym w punkcie 5.7.4 niniejszego Kodeksu Postępowania Certyfikacyjnego.

EID wymaga uprzedniej autoryzacji posiadacza przed przystąpieniem do publikacji zaświadczenia.

2.2. Publikacja informacji dostawcy usług certyfikacji elektronicznej

EID publikuje w swoim Repozytorium następujące informacje:

- Wydane certyfikaty.
- Listy unieważnionych certyfikatów i inne informacje o statusie unieważnionych certyfikatów.
- Obowiązujące zasady dotyczące certyfikatów.
- Oświadczenie o praktykach certyfikacyjnych

Wszelkie zmiany specyfikacji lub warunków usługi będą komunikowane użytkownikom przez Urząd Certyfikacji poprzez stronę internetową.

2.3. Częstotliwość publikacji.

Informacje o dostawcy usług certyfikacyjnych oraz zasady i Kodeks Postępowania Certyfikacyjnego, są publikowane od razu po ich udostępnieniu.

Zmiany w Kodeksie Postępowania Certyfikacyjnego kierują się postanowieniami punktu 1.5 niniejszego dokumentu.

Informacja o statusie unieważnienia certyfikatów jest publikowana zgodnie z postanowieniami pkt. 4.9.9 i 4.9.10 niniejszego Kodeksu Postępowania Certyfikacyjnego.

2.4. Kontrola dostępu do repozytoriów

EID nie ogranicza dostępu do odczytu informacji wymienionych w punkcie 2.2. ale ustanawia środki kontroli zapobiegające dodawaniu, modyfikowaniu lub usuwaniu rejestrów z repozytorium przez osoby nieupoważnione, w celu ochrony integralności i autentyczności informacji, w szczególności informacji o stanie unieważnień.

EID stosuje zaufane systemy dla Repozytorium w taki sposób, aby:

- Tylko upoważnione osoby mogły dokonywać adnotacji i modyfikacji
- Było możliwe zweryfikować autentyczności informacji
- Certyfikaty były dostępne do wglądu tylko wtedy, gdy osoba fizyczna wskazana w certyfikacie wyraziła na to zgodę.
- Było możliwe wykryć wszelkie zmiany techniczne wpływające na wymagania bezpieczeństwa.

3. Identyfikacja i uwierzytelnianie

3.1. Identyfikacja

3.1.1. Rodzaje nazw

Wszystkie certyfikaty zawierają nazwę wyróżniającą (DN lub distinguished name) zgodną ze standardem X.501 w polu Subject, w tym element Common Name (CN=) odnoszący się do tożsamości użytkownika i osoby fizycznej zidentyfikowanej w certyfikacie, a także różne dodatkowe informacje o tożsamości w polu SubjectAlternativeName.

Nazwy zawarte w certyfikatach są następujące.

Certyfikat kwalifikowany Osoby Fizycznej w CHMURZE bez QSCD

Country (C)	Państwo[1]
Surname	Nazwisko osoby podpisującej
Given Name	Imię osoby podpisującej
Serial Number	Dowód osobisty/ Paszport/ lub inny odpowiedni numer identyfikacyjny podpisującego, uznawany przez prawo
Common Name (CN)	Imię i nazwisko osoby podpisującej

Certyfikat kwalifikowany Osoby Fizycznej w CHMURZE z QSCD

Country (C)	Państwo[2]
Surname	Nazwisko osoby podpisującej
Given Name	Imię osoby podpisującej
Serial Number	Dowód osobisty / Paszport / lub inny odpowiedni numer identyfikacyjny osoby podpisującej uznawany przez prawo
Common Name (CN)	Imię i nazwisko osoby podpisującej

3.1.2. Znaczenie nazw

Nazwy znajdujące się w polach SubjectName i SubjectAlternativeName są zrozumiałe w języku naturalnym, jak ustalono w poprzedniej sekcji.

Jeżeli dane wskazane w CN lub Podmiocie są fałszywe lub wyraźnie wskazano, że certyfikat jest nieważny, uważa się, że nie ma on mocy prawnej dlatego też nie ma odpowiedzialności za TSP,

1 Pole „Państwo" będzie odpowiadało państwu, w którym występuje stosunek umowny między podpisującym a podmiotem, z którym jest powiązany (ponieważ jest pracownikiem, członkiem, partnerem lub innym łącznikiem), niezależnie od narodowości pracownika.

2 Pole „Państwo" będzie odpowiadało państwu, w którym występuje stosunek umowny między podpisującym a podmiotem, z którym jest powiązany (ponieważ jest pracownikiem, członkiem, partnerem lub innym łącznikiem), niezależnie od narodowości pracownika.

ponieważ certyfikaty te są wydawane w celu przeprowadzenia testów technicznych i oceny podmiotu regulacyjnego.

3.1.3. Zastosowanie anonimowości lub pseudonimów

Pod żadnym względem nie można używać pseudonimów do identyfikacji danej jednostki, firmy lub organizacji, ani podpisującego. Również pod żadnym względem nie wydaje się anonimowych zaświadczeń.

3.1.4. Interpretacja formatów nazw

Formaty nazw będą interpretowane zgodnie z prawem kraju siedziby użytkownika, na własnych warunkach.

Pole „państwo" lub „stan" będzie polem użytkownika certyfikatu.

Pole „serial number" zawiera numer dokumentu, Paszport lub inny odpowiedni numer identyfikacyjny podpisującego, uznany przez prawo.

3.1.5. Niepowtarzalność nazw

Nazwy użytkowników są niepowtarzalne.

Używana już nazwa użytkownika nie może być przypisana innemu użytkownikowi, co z zasady nie powinno mieć miejsca ze względu na obecność w schemacie nazewniczym numeru NIP lub jego odpowiednika.

Użytkownik może zażądać więcej niż jednego certyfikatu, pod warunkiem, że kombinacja następujących wartości w żądaniu różni się od ważnego już certyfikatu:

- Numer Identyfikacji Podatkowej (NIF) lub inny prawnie ważny numer identyfikacyjny osoby fizycznej.
- Numer Identyfikacji Podatkowej (CIF/NIF) lub inny prawnie ważny identyfikator użytkownika.
- Rodzaj certyfikatu (identyfikator polityki certyfikatu OID).
- Obsługa certyfikatów (QSCD, oprogramowanie, scentralizowany HSM, scentralizowany QSCD)

W drodze wyjątku niniejszy Kodeks dopuszcza wydawanie certyfikatu, gdy CIF/NIF osoby podpisującej, NIF podpisującego, Typ certyfikatu i Obsługa certyfikatu pokrywają się z aktywnym certyfikatem, pod warunkiem, że istnieje jakiś element, który je różni w ładunku (tytuł) i/lub dziale (Organizational Unit).

3.2. Weryfikacja tożsamości

Tożsamość użytkowników certyfikatu ustalana jest w momencie podpisania umowy pomiędzy EID a użytkownikiem w momencie kiedy istnienie użytkownika weryfikowane jest za pomocą urzędowego dokumentu tożsamości.

3.2.1. Sprawdzanie posiadania klucza prywatnego

O posiadaniu klucza prywatnego świadczy rzetelna procedura dostarczenia i akceptacji certyfikatu przez subskrybenta w certyfikatach pieczęci lub przez podpisującego w certyfikatach podpisu.

3.2.2. Weryfikacja tożsamości

Wydając kwalifikowany certyfikat dla usługi zaufania, EID zweryfikuje, za pomocą odpowiednich środków i zgodnie z prawem krajowym, tożsamość oraz, w stosownych przypadkach, wszelkie szczególne atrybuty osoby fizycznej lub prawnej, której wydawany jest kwalifikowany certyfikat. Tożsamość osoby fizycznej wskazanej w certyfikacie musi być skrupulatnie potwierdzona, dlatego w momencie wystawiania certyfikatu tożsamość osoby podpisującej jest akredytowana przed operatorem rejestru, weryfikując ją poprzez przedstawienie dokumentów lub poprzez źródła własne, zachowując ich ważności.

Wtedy EID zweryfikuje informacje bezpośrednio lub za pośrednictwem osoby trzeciej zgodnie z prawem krajowym:

a) w obecności osoby fizycznej, dla której użytkownik musi stawić się w biurach EID pod adresem Av. de la Ciudad de Barcelona, 81, 4, 28007 Madryt, ponieważ nie ma delegowanych Organów Rejestracji;

b) zdalnie, za pomocą środków identyfikacji elektronicznej zgodnie z postanowieniami Rozporządzenia ETD/465/2021 z dnia 6 maja, które reguluje metody zdalnej identyfikacji wideo w celu wydawania kwalifikowanych certyfikatów elektronicznych.

c) za pomocą certyfikatu kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej wystawionej zgodnie z lit. a) lub b), lub;

Dokumentowe uzasadnienie powiązania osoby fizycznej wskazanej w certyfikacie z podmiotem związane jest z jej wpisem w rejestrze wewnętrznym podmiotu.

Niezależnie od powyższego, weryfikacja tożsamości nie będzie wymagana, gdy tożsamość lub inne stałe okoliczności podpisujących, którym wydawane są certyfikaty, pojawiają się już w EID na mocy istniejącego wcześniej związku, o ile do identyfikacji osobistej podpisującego -została zastosowana metoda identyfikacji bezpośredniej i minęło nie więcej niż 5 lat.

3.2.3. Uwierzytelnienie tożsamości osoby fizycznej

Tożsamość wnioskującego o wydanie certyfikatu oraz tożsamość osób fizycznych podpisujących wskazanych w certyfikatach będą sprawdzane i potwierdzane przez operatora lub upoważniony personel Punktu Rejestracji EID, działając w następujący sposób:

- Gdy identyfikacja została dokonana osobiście, poprzez sprawdzenie:
  - Dostarczony dokument identyfikacyjny.
- Gdy identyfikacja została dokonana za pomocą metody identyfikacji elektronicznej poprzez identyfikację wideo EID, w procesie określonym w sekcji 3.2.4 niniejszego dokumentu poprzez:
  - Przegląd wideo i zdjęć zarejestrowanych dostarczonego dokumentu tożsamości wnioskodawcy.
  - Potwierdzenie dowodu życia wnioskodawcy na podstawie wyników dostarczonych przez zdalny system identyfikacji wideo.
  - Przegląd porównania wykonanego przez system zdalnej identyfikacji wideo zdjęcia dokumentu tożsamości z obrazami i wideo uzyskanymi podczas rejestracji wnioskodawcy.
  - Przegląd stworzony przez system zdalnej identyfikacji wideo, za pomocą sztucznej inteligencji do wykrywania fałszywych dokumentów tożsamości.

3.2.4. Nieweryfikowana informacja o użytkowniku.

EID nie zawiera żadnych niezweryfikowanych danych subskrybenta w certyfikatach.

3.2.5. Uwierzytelnianie tożsamości podmiotu rejestrującego i jego operatorów

W przypadku powiązania nowego podmiotu rejestrującego należy przeprowadzić potrzebne weryfikacje, aby potwierdzić istnienie danego podmiotu lub organizacji, w tym celu można wykorzystać wystawienie dokumentów lub wykorzystanie źródeł w własnych informacji.

W ten sam sposób, bezpośrednio lub za pośrednictwem punktu rejestracji, należy zweryfikować tożsamość operatorów punktów rejestracji, przesyłając odpowiednią dokumentację identyfikacyjną, a także ich upoważnienie do działania.

Operatorzy Punktu Rejestracji muszą mieć zapewnione odpowiednie przeszkolenie do wykonywania swoich funkcji, dlatego też należy oceniać ich w tym celu.

3.2.6. Weryfikacja tożsamości drogą elektroniczną

Proces Identyfikacji wideo lub wideokonferencja asynchroniczna (zwany dalej „Procesem Identyfikacji Wideo" lub „Procesem") to zdalna metoda weryfikacji tożsamości wideo w czasie rzeczywistym, która rejestruje cały proces rejestracji osoby i pozwala na zdalną weryfikację dokumentów tożsamości, za pomocą nagrania wideo, które rejestruje i weryfikuje dokument tożsamości w czasie rzeczywistym i w sposób zautomatyzowany (około 10-20 sekund), co jest przeprowadzane przez EID za pośrednictwem ich operatorów weryfikacji.

Proces składa się z dwóch etapów, automatycznego modułu, w którym przeprowadzana jest wielokrotna kontrola elementów zabezpieczających dokument pokazany podczas nagrywania wideo, a także biometrycznego porównania twarzy osoby przedstawiającej dokument użytkownika oraz jego zdjęcie, wykonując wtedy dowód życia i wyodrębnienie danych w precyzyjny sposób.

Te informacje służą jako element wspierający decyzję agenta ludzkiego z urzędu rejestracji, który następnie dokona przeglądu pełnego nagrania wideo (asynchronicznie), określając, czy można potwierdzić tożsamość na podstawie przedstawionych dowodów, czy nie.

Technologia weryfikuje autentyczność dokumentów tożsamości, w tym kontrole bezpieczeństwa w czasie rzeczywistym, takie jak wykrywanie hologramów, identyfikatorów, wzorów i innych elementów zabezpieczających dokument.

3.2.6.1. Opis procesu wideo identyfikacji

Proces identyfikacji wideo opracowywany jest według następujących elementów:

- Wskazówki głosowe i tekstowe podczas procesu identyfikacji wideo.
- Zautomatyzowana kontrola elementów otoczenia (warunki oświetlenia, sieć, jakość kamer) pozwalająca na uzyskanie optymalnego zapisu identyfikacji wideo i jej ewidencji.
- Porównanie obrazów z oryginalnymi dokumentami za pomocą technologii *pattern matching* w celu weryfikacji autentyczności dokumentu.
- Wydobycie danych (OCR) z MRZ lub innych części dokumentu oraz możliwość wywołania poświadczeń w czasie rzeczywistym.
- Weryfikacja faktu, że przód i tył dokumentu należą do tego samego dokumentu.
- Rejestracja biometryczna osoby i porównanie w czasie rzeczywistym z wizerunkiem dokumentu tożsamości.
- Narzędzie do Weryfikacji Urzędu Rejestracji umożliwiające przegląd procesu przez wykwalifikowanego człowieka, który został wcześniej wykwalifikowany w ramach specjalnego szkolenia.

Oznacza to że, gdy użytkownik wybierze dokument, którego zamierza użyć do przeprowadzenia procesu, strumieniowe nagranie wideo będzie kontrolowane przez aplikację, w której ten proces zostanie uruchomiony i w której użytkownik pokaże przód i tył dokumentu w celu identyfikacji i weryfikacji w czasie rzeczywistym. Ponadto użytkownik zostanie również poproszony o pokazanie swojej twarzy w procesie rozpoznawania twarzy w oparciu o automatyczną punktację biometryczną, w tym wykrywanie życia, prosząc użytkownika o interakcję ruchem i wydobywając dane z dokumentu przez OCR.

W przypadku asynchronicznej weryfikacji przez agenta ludzkiego istnieje protokół bezpieczeństwa oparty na dobrych praktykach UE, który jest wspomagany przez narzędzie oferowane agentowi ludzkiemu, w którym pokazane są dowody uzyskane podczas procesu, a także flagi lub powiadomienia o nieotrzymanych. Cały proces jest śledzony ze znacznikiem czasu przy każdym postępie.

To oznacza, że system zapewnia szereg potwierdzeń weryfikacji od dowodów zebranych przez Automatyczny Proces Wideo do śladów łączących identyfikację z wykwalifikowanym agentem punktu rejestracji. W ten sposób wynikiem jest zweryfikowana tożsamość, której zabezpieczenia techniczne są tak samo ważne jak zabezpieczenia przeprowadzane osobiście.

3.2.6.2. Obowiązki użytkownika w związku z procesem identyfikacji wideo

Użytkownik przez cały proces zobowiązuje się do:

- Korzystania z Usługi zgodnie z postanowieniami Warunków Procesu Identyfikacji Wideo i wystawiania kwalifikowanych certyfikatów, w Kodeksie Postępowania Certyfikacyjnego, w szczególnych warunkach, które mogą mieć zastosowanie oraz z wszelkimi innymi instrukcjami lub procedurą przez EID.

- Dokument użyty w procesie jest dokumentem autentycznym, prawnie ważnym oraz że dodatkowo:

    - Nie jest to kserokopia ani drukowana karta:
    - Nie jest w formacie cyfrowym (telefon komórkowy, tablet lub komputer).
    - Nie jest w pokrowcu.
    - Nie jest uszkodzony i jest kompletny, ze wszystkimi zabezpieczeniami dokumentu.

- Że podczas procesu i przechwytywania wideo, aby nie został odrzucony:

- Warunki oświetleniowe podczas wideo muszą umożliwiać dobrą widoczność twarzy zidentyfikowanej osoby i dokumentu.
- Wideo musi mieć stały przepływ, bez cięć i opóźnień.
- Żyjąca osoba musi okazać dowód tożsamości.
- Jeżeli inna osoba niż osoba, która ma zostać zidentyfikowana, przeprowadza cały proces, identyfikacja zostanie odrzucona.
- Jeśli podczas wideo rozmowy jest obecna inna osoba, ale wyraźnie nie zmusza tej osoby do identyfikacji, identyfikacja może być ważna, tak jak w przypadku, gdy dana osoba pomaga osobie niepełnosprawnej w dokonaniu identyfikacji.
- Muszą być wyraźnie widoczne wszystkie części uchwyconego dokumentu, przodu, tyłu i twarzy osoby.
- Użytkownik nie może spać ani wykazywać oznak, które mogłyby zostać zinterpretowane jako stan nietrzeźwości bądź odurzenia.

3.2.6.3. Okres przechowywania informacji

Wszystkie informacje związane z procesem identyfikacji wideo i wydawaniem kwalifikowanych certyfikatów elektronicznych w procesie identyfikacji wideo tożsamości, w tym informacje biometryczne, będą przechowywane przez okres trwania stosunku umownego, o ile ich usunięcie nie jest wymagane. Oraz w okresie przedawnienia mogących powstać z czynności prawnych lub roszczeń, które mogą otrzymać organy urzędowe.

Maksymalny okres przechowywania kluczowych danych związanych z procesem wideo identyfikacji i wydawania kwalifikowanych certyfikatów wyniesie 15 lat od momentu wydania certyfikatu, chyba że przepisy w prawie stanowią inaczej. Po zakończeniu relacji dane zostaną należycie zablokowane, zgodnie z postanowieniami obowiązujących przepisów. Ponadto zgłasza się, że wszystkie dowody niekompletnych procesów identyfikacji, które nie zostały ukończone z powodu podejrzenia próby oszustwa, będą przechowywane przez okres 5 lat od wykonania procesu, z wyszczególnieniem przyczyny ich niedokończenia. Zgodnie z ustanowioną w tym celu polityką.

3.3. Identyfikacja i uwierzytelnianie wniosków o odnowienie

3.3.1. Identyfikacja i uwierzytelnianie w celu rutynowego odnawiania

Przed odnowieniem certyfikatu operator lub upoważniony personel sprawdza, czy informacje służące do weryfikacji tożsamości oraz inne dane użytkownika i osoby fizycznej zidentyfikowanej w certyfikacie są nadal aktualne.

Śledczoperator lub upoważniony personel Punktu Rejestracji uwierzytelnia wnioski i zgłoszenia związane z unieważnieniem, zawieszeniem lub ponowną aktywacją certyfikatu, weryfikując, czy pochodzą od osoby upoważnionej.

Identyfikacja użytkowników lub podpisujących w procesie unieważniania, zawieszania lub reaktywacji certyfikatów może odbywać się poprzez:

Użytkownik lub podpisujący:

- Identyfikacja i uwierzytelnianie za pomocą kodu odwołania (ERC lub ERC) za pośrednictwem strony internetowej UANATACA 24x7. Stosowanie kodu „CRE" lub „ERC" związanego z poprzednim certyfikatem lub innych metod uwierzytelniania osobistego, na które składa się informacja, którą zna tylko osoba fizyczna zidentyfikowana w certyfikacie i która umożliwia automatyczne odnowienie certyfikatu, pod warunkiem że maksymalny określony prawnie termin nie został przekroczony.
- Inne środki komunikacji, takie jak telefon, e-mail itp. gdy istnieją uzasadnione gwarancje tożsamości wnioskodawcy o zawieszenie lub cofnięcie, w opinii EID i/lub Organów Rejestracji.

Organy rejestracji EID: muszą zidentyfikować osobę podpisującą przed złożeniem wniosku o unieważnienie, zawieszenie lub reaktywację w sposób, jaki uznają za niezbędny.

Gdy użytkownik chce złożyć wniosek o unieważnienie w godzinach pracy a istnieją wątpliwości co do jego identyfikacji, jego certyfikat przechodzi w stan zawieszenia.

Jedną z metod weryfikacji statusu certyfikatów jest zapoznanie się z najnowszą listą unieważnionych certyfikatów wydaną przez urząd certyfikacji EID.

Listy unieważnionych certyfikatów są publikowane w Repozytorium Urzędów Certyfikacji, a także pod następującymi adresami internetowymi, wskazanymi wewnątrz certyfikatów:

- http://crl1.uanataca.com/public/pki/crl/eid.crl
- http://crl2.uanataca.com/public/pki/crl/eid.crl

Status ważności certyfikatów można również sprawdzić za pomocą protokołu OCSP.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

3.3.2. Identyfikacja i uwierzytelnienie wniosku o odnowienie

Przed dokonaniem odnowienia upoważniony personel Punktu Rejestracji musi zweryfikować, czy informacje wykorzystywane w tym czasie do weryfikacji tożsamości oraz pozostałe dane użytkownika i osoby fizycznej zidentyfikowanej w poprzednim certyfikacie są nadal aktualne.

Odnowienie certyfikatów po unieważnieniu nie będzie możliwe w następujących przypadkach:

- Omyłkowo unieważniony certyfikat osobie innej niż wskazana w certyfikacie.
- Unieważnienie certyfikatu z powodu nieuprawnionego wydania przez wskazaną w certyfikacie osobę fizyczną.
- Certyfikat z błędnymi lub fałszywymi informacjami.

W przypadku zmiany danych użytkownika lub osoby fizycznej wskazanej w certyfikacie, nowe informacje są odpowiednio rejestrowane więc stworzona jest kompletna identyfikacja.

3.4. Identyfikacja i uwierzytelnienie wniosku o unieważnienie

Śledczy, operator lub upoważniony personel Punktu Rejestracji uwierzytelnia wnioski i zgłoszenia związane z unieważnieniem, zawieszeniem lub ponowną aktywacją certyfikatu, weryfikując, czy pochodzą od osoby upoważnionej.

Identyfikacja użytkowników lub podpisujących w procesie unieważniania, zawieszania lub reaktywacji certyfikatów może odbywać się poprzez:

- Użytkownik lub podpisujący:
  - Identyfikacja i uwierzytelnianie za pomocą kodu odwołania (ERC lub ERC) za pośrednictwem strony internetowej UANATACA 24x7.
  - Inne środki komunikacji, takie jak telefon, e-mail itp., gdy istnieją uzasadnione gwarancje tożsamości wnioskodawcy o zawieszenie lub cofnięcie, w opinii EID i/lub Organów Rejestracji.
- Organy rejestracji EID: muszą zidentyfikować podpisującego przed złożeniem wniosku o unieważnienie, zawieszenie lub reaktywację w sposób, jaki uznają za niezbędny.

Gdy użytkownik chce złożyć wniosek o unieważnienie w godzinach pracy a istnieją wątpliwości co do jego identyfikacji, jego certyfikat przechodzi w stan zawieszenia.

4. Wymagania dotyczące cyklu życia certyfikatu

4.1. Certyfikaty krótkoterminowe

4.1.1. Wniosek o wydanie certyfikatu krótkoterminowego

Proces ubiegania się o certyfikat może odbywać się zarówno za pośrednictwem EID, jak i za pośrednictwem osób trzecich o charakterze publicznym lub prywatnym, z którymi EID zawarł określone porozumienia umowne.

W przypadku, gdy wnioskodawca za pośrednictwem EID lub za pośrednictwem osób trzecich wskazanych powyżej wystąpi o wydanie certyfikatu, EID prześle e-mail potwierdzający wydanie certyfikatu i rozpoczęcie Procesu Identyfikacji zgodnie z postanowieniami pkt. 3.2. 4 niniejszego dokumentu (na potrzeby pkt 4.1, zwanego dalej procesem identyfikacji), a także przekazywania informacji związanych z niezbędną wcześniejszą konfiguracją związaną z procesem akredytacji tożsamości na odległość oraz wydaniem i korzystaniem z certyfikatu wykwalifikowanej osoby fizycznej. W tym procesie wnioskodawca otrzyma przez pocztę elektroniczną link do rozpoczęcia Procesu Identyfikacji.

4.1.1.1. Legitymacja do wniosku o wydanie certyficatu

Wnioskodawca wchodząc za pośrednictwem linku przyjmuje wniosek o wydanie certyfikatu oraz dodatkowo musi zapoznać się i wyraźnie zaakceptować warunki procesu identyfikacji poprzez zaznaczenie w tym celu wyświetlonego okienka. Zaznaczenie tego okienka (checkbox) przez wnioskodawcę będzie traktowane jako zwykły podpis.

4.1.2. Proces wniosku o certyfikację

4.1.2.1. Wykonywanie działań potrzebnych do identyfikacji i uwierzytelnienia

Przed wysłaniem wiadomości e-mail do wnioskodawcy, EID wygeneruje kod identyfikacyjny, który zostanie wysłany do wnioskodawcy we wspomnianej wiadomości elektronicznej w celu powiązania procesu identyfikacji z konkretnym wnioskiem wnioskodawcy o wydanie certyfikatu.

Gdy wnioskodawca uzyskuje dostęp do systemu identyfikacji wideo za pośrednictwem linku podanego w wiadomości e-mail, EID zweryfikuje, czy podany kod identyfikacyjny odpowiada żądaniu identyfikacji i, jeśli jest poprawny, umożliwi rozpoczęcie procesu identyfikacji za pomocą Aplikacji EID.

W procesie identyfikacji zostaną uzyskane niezbędne informacje do umieszczenia w certyfikacie, poprzez informacje zawarte w dokumencie tożsamości używanym do przeprowadzenia tego procesu. Jeżeli proces identyfikacji jest prawidłowy i tożsamość wnioskodawcy zostanie potwierdzona, EID zatwierdzi wniosek o wydanie certyfikatu i przystąpi do jego wydania zgodnie z postanowieniami niniejszego oświadczenia o praktyce certyfikacyjnej.

Dokumentacja uzasadniająca zatwierdzenie wniosku musi być przechowywana i należycie rejestrowana oraz z gwarancjami bezpieczeństwa i integralności przez okres 15 lat

od wygaśnięcia certyfikatu, nawet w przypadku wcześniejszej utraty ważności z powodu unieważnienia.

4.1.2.2. Zaakceptowanie lub odrzucenie wniosku

Po zakończeniu procesu identyfikacji wnioskodawca nie wychodząc z aplikacji będzie czekał na potwierdzenie tożsamości przez ludzkiego agenta weryfikacji. W przypadku, gdy proces identyfikacji przebiegnie prawidłowo i zostanie potwierdzona tożsamość Wnioskodawcy, proces wydawania certyfikatu będzie kontynuowany. W tym momencie, w celu kontynuacji procesu wydawania certyfikatu, wnioskodawca musi wyraźnie zaakceptować ogólne warunki świadczenia usługi certyfikacji elektronicznej dla certyfikatów kwalifikowanych krótkoterminowych oraz Kodeks Postępowania Certyfikacyjnego poprzez zaznaczenie odpowiednich pól wyboru . Oznaczenie tych pól weryfikacyjnych przez wnioskodawcę będzie traktowane jako zwykły podpis.

W przypadku, gdy tożsamość wnioskodawcy nie zostanie akredytowana, zostanie on o tym poinformowany za pośrednictwem aplikacji, a w konsekwencji akredytacja procesu identyfikacji zostanie odrzucona, a tym samym nie będzie możliwe kontynuowanie procesu wniosku o wydanie certyfikatu.

4.1.3. Wydanie certyfikatu

4.1.3.1. Działanie CA podczas procesu wydania

Zatwierdzony wniosek certyfikacyjny przez EID wydawany jest w bezpieczny sposób. Podczas procesu EID musi zająć się szeregiem zadań:

- Chroni poufność i integralność posiadanych danych rejestracyjnych.
- Korzysta z niezawodnych systemów i produktów, które są zabezpieczone przed wszelkimi zmianami i gwarantują bezpieczeństwo techniczne oraz w tym przypadku, kryptograficzne bezpieczeństwo obsługiwanych przez nie procesów certyfikacji.
- Generuje parę kluczy za pomocą procedury generowania certyfikatu, bezpiecznie połączonej z procedurą generowania kluczy.
- Wykorzystuje procedurę generowania certyfikatu, która bezpiecznie łączy certyfikat z informacjami rejestracyjnymi, w tym z certyfikowanym kluczem publicznym.
- Gwarantuje, że certyfikat jest wystawiany przez system stosujący zabezpieczenia przed fałszerstwem oraz gwarantujące poufność kluczy podczas procesu generowania ich.
- Podaje datę i godzinę wydania certyfikatu, dokumencie certyfikatu.
- Gwarantuje wyłączną kontrolę nad kluczami przez użytkownika, a sam EID ani jego Punkty Rejestracji nie mogą ich w żaden sposób wydedukować ani wykorzystać.

4.1.4. Wydanie i zaakceptowanie poprzez używanie certyfikatu

W procesie wydawania certyfikatu krótkoterminowego nie ma żadnej specyficznej formy dostarczenia certyfikatu wnioskodawcy, sam wnioskodawca użyje certyfikatu podczas tego samego procesu do elektronicznego podpisywania dokumentów, kończąc jego ważność po jednorazowym użytku, w każdym razie maksymalny okres użytkowania nie może przekroczyć 24 godzin.

Podczas tego procesu upoważniony operator EID lub personel musi wykonać następujące czynności:

- Udokumentować definitywnie tożsamość osoby fizycznej wskazanej w certyfikacie, zgodnie z postanowieniami tego dokumentu.
- Zapewnienie świadczenia usług certyfikacyjnych należycie podpisanych i zaakceptowanych drogą elektroniczną przez użytkownika, a także zachowanie wszelkich czynów użytkownika dotyczących pozytywnej manifestacji w odpowiednich polach wyboru.
- Po wydaniu certyfikatu i podpisaniu dokumentów elektronicznie doręczyć, dokument, w którym identyfikuje się dane dostawcy usług certyfikacyjnych, indywidualnego użytkownika certyfikatu, dane identyfikacyjne użytkownika i osoby podpisującej dokumenty, datę i godzinę, dokumenty podpisane elektronicznie oraz informacje o zdarzeniach, które miały miejsce w procesie wydawania certyfikatu.
- W niektórych przypadkach, w zależności od rodzaju wydanego certyfikatu, potwierdzenie dostawy i odbioru certyfikatu do osoby fizycznej wskazanej w certyfikacie, z następującą minimalną treścią:

Akceptacja certyfikatu nastąpi podczas używania go.

4.1.5. Stosowanie certyfikatu: Używanie kluczy publicznych i prywatnych

4.1.5.1. Używanie przez odbiorcę

Aby wnioskodawca mógł posługiwać się certyfikatem elektronicznym oraz kluczami publicznymi i prywatnymi, EID przeprowadzi następujące czynności:

- Wygenerowanie krótkoterminowego certyfikatu elektronicznego użytkownika, aby mógł służyć do podpisywania dokumentów elektronicznych dostarczonych przez osoby trzecie, podczas procesu podpisywania. Wtedy EID umożliwią mechanizmy techniczne, dzięki którym użytkownik będzie mógł uzyskać dostęp do swojego certyfikatu online i podpisywać dokumenty elektronicznie.

- Wygenerowany certyfikat elektroniczny oraz klucze publiczny i prywatny będą przechowywane przez EID jako Kwalifikowany Dostawca Usług Zaufania.
- W celu przeprowadzenia procesu podpisywania, użytkownik otrzyma kod OTP na podany wcześniej przez nie numer telefonu, dzięki czemu kod ten będzie pod wyłączną kontrolą użytkownika.
- Jednocześnie użytkownik będzie miał dostęp do przeglądu dokumentu do podpisania. Jeżeli użytkownik będzie chciał podpisać dokumenty, będzie musiał je przeczytać i wyraźnie zaakceptować oraz podać kod OTP wydany przez EID za pośrednictwem aplikacji.
- W momencie podpisywania dokumentów użytkownik podaje kod OTP nadany za pomocą aplikacji EID. Za pomocą tego kodu EID, działając jako kwalifikowany dostawca usług zaufania, zastosuje klucz prywatny użytkownika i podpisze dokument.
- Po podpisaniu dokumentu w formie elektronicznej i upływie okresu jego ważności certyfikat traci ważność bez możliwości ponownego wykorzystania przez użytkownika.

4.1.5.2. Użycie przez osoby trzecie, które ufają w certyfikaty.

EID informuje osobę trzecią, która ufa certyfikatom, że musi przyjąć następujące obowiązki:

- Doinformować się, czy certyfikat jest odpowiedni do zamierzonego zastosowania.
- Zweryfikować ważność, zawieszenie lub unieważnienie wydanych certyfikatów, do czego będzie wykorzystywał informacje o statusie certyfikatów.
- Zweryfikować wszystkie certyfikaty w hierarchii certyfikatów, zanim zaufa podpisowi cyfrowemu lub innemu z certyfikatów w hierarchii.
- Uznać, że zweryfikowane podpisy elektroniczne złożone w kwalifikowanym urządzeniu do tworzenia podpisów (DCCF) są prawnie uważane za kwalifikowane podpisy elektroniczne; czyli odpowiednik podpisów odręcznych, a także fakt, że certyfikat umożliwia tworzenie innych rodzajów podpisów elektronicznych i mechanizmów szyfrowania.
- Należy pamiętać o wszelkich ograniczeniach dotyczących korzystania z certyfikatu, niezależnie od tego, czy znajduje się ono w samym certyfikacie, czy w umowie strony trzeciej, która ufa certyfikatowi.

- Uwzględnić wszelkie środki ostrożności ustanowione w umowie lub innym instrumencie, niezależnie od ich charakteru prawnego.
- Nie monitorować, nie manipulować ani nie przeprowadzać czynności inżynierii wstecznej w zakresie technicznym realizacji usług certyfikacji EID bez uprzedniej pisemnej zgody.
- Nie narażać bezpieczeństwa usług certyfikacji EID.

4.1.6. Odnawiać klucze i certyfikaty

Nie dotyczy.

4.1.7. Modyfikacja certyfikatów

Nie dotyczy.

4.1.8. Unieważnienie, zawieszenie lub reaktywacja certyfikatów

Unieważnienie certyfikatu zakłada definitywną utratę jego ważności i jest nieodwracalne.

Zawieszenie (lub czasowe unieważnienie) certyfikatu oznacza utratę jego tymczasowej ważności i jest odwracalne. Tylko certyfikaty podmiotu końcowego mogą podlegać zawieszeniu.

Reaktywacja certyfikatu zakłada jego przejście ze statusu zawieszonego do statusu aktywnego.

4.1.9. Powody unieważnienia certyfikatu

EID odwołuje certyfikat, gdy wystąpi jedna z następujących przyczyn:

1) Okoliczności wpływające na informacje zawarte w certyfikacie:

a) Modyfikacja jakichkolwiek danych zawartych w certyfikacie, po odpowiednim wydaniu certyfikatu zawierającego modyfikacje.
b) Odkrycie, że pewne dane zawarte we wniosku certyfikatu są nieprawidłowe.
c) Odkrycie, że niektóre dane zawarte w certyfikacie są nieprawidłowe.

2) Okoliczności wpływające na bezpieczeństwo klucza lub certyfikatu:

a) Naruszenie klucza prywatnego, infrastruktury lub systemów dostawcy usług certyfikacyjnych, który wystawił certyfikat, o ile wpływa na wiarygodność certyfikatów wydanych w wyniku tego incydentu.
b) Naruszenie przez EID wymagań określonych w procedurach zarządzania certyfikatami, określonych w niniejszym Kodeksie Postępowania Certyfikacyjnego.

c) Naruszenie lub podejrzenie naruszenia bezpieczeństwa klucza lub wydanego certyfikatu.
d) Nieautoryzowany dostęp lub użycie przez stronę trzecią klucza prywatnego odpowiadającego kluczowi publicznemu zawartemu w certyfikacie.
e) Niepoprawne użycie certyfikatu przez wskazaną w certyfikacie osobę fizyczną lub brak sumienności w przechowywaniu klucza prywatnego.

3) Okoliczności mające wpływ na użytkownika lub wskazaną w certyfikacie osobę fizyczną:

a) Rozwiązanie stosunku prawnego o świadczenie usług pomiędzy EID a użytkownikiem.
b) Zmiana lub rozwiązanie istniejącego stosunku prawnego lub przyczyny, która spowodowała wydanie certyfikatu wskazanej w certyfikacie osobie fizycznej.
c) Naruszenie przez wnioskodawcę certyfikatu wcześniej ustalonych wymogów dla jego wniosku
d) Naruszenie przez użytkownika lub osobę wskazaną w certyfikacie ich zobowiązań, odpowiedzialności i gwarancji określonych w odpowiednim dokumencie prawnym.
e) Nagła niepełnosprawność lub śmierć posiadacza klucza.
f) Wniosek użytkownika o unieważnienie certyfikatu, zgodnie z postanowieniami pkt.

4) Inne okoliczności

a) Zakończenie usługi certyfikacyjnej Jednostki Certyfikującej EID.
b) Używanie certyfikatu, które jest szkodliwe i jest kontynuowane dla EID. W takim sytuacji użycie go uważa się za szkodliwe względem następujących kryteriów:

- Specyfika oraz ilość otrzymanych skarg.
- Tożsamość podmiotów składających reklamacje
- Odpowiednie przepisy obowiązujące w danym czasie.
- Odpowiedź użytkownika lub osoby wskazanej w certyfikacie na otrzymane reklamacje.

4.1.10. Powody zawieszenia certyfikatu

Certyfikaty EID mogą zostać zawieszone z następujących powodów:

- Na żądanie użytkownika lub osoby fizycznej wskazanej w certyfikacie.
- Gdy dokumentacja wymagana we wniosku o unieważnienie jest wystarczająca, ale nie można dorzecznie zidentyfikować użytkownika lub osoby fizycznej wskazanej w certyfikacie.
- Nieużywanie certyfikatu przez długi czas, wcześniej znany.
- W przypadku podejrzenia o włamanie do klucza, do czasu jego potwierdzenia. W takim przypadku EID musi zadbać o to, aby certyfikat nie był zawieszony na dłużej niż jest to konieczne do potwierdzenia swojego zobowiązania.

4.1.11. Przyczyny reaktywacji certyfikatu

Świadectwa EID można reaktywować z następujących powodów:

- Gdy certyfikat jest w stanie zawieszenia.
- Na żądanie użytkownika lub osoby fizycznej wskazanej w certyfikacie.

4.1.12. Kto może ubiegać się o unieważnienie, zawieszenie lub reaktywacje

Mogą wystąpić o unieważnienie, zawieszenie lub reaktywację certyfikatu:

- Osoba wskazana w certyfikacie.
- Użytkownik certyfikatu za pośrednictwem podmiotu odpowiedzialnego za usługę certyfikacyjną.

4.1.13. Proces wnioskowania o unieważnienie, zawieszenie lub reaktywacje

Podmiot, który potrzebuje unieważnienia, zawieszenia lub reaktywacji certyfikatu, może zwrócić się o to bezpośrednio do EID albo Punktu Rejestracji użytkownika lub zrobić to samodzielnie za pośrednictwem serwisu internetowego dostępnego na stronie EID.

Wniosek o unieważnienie, zawieszenie lub reaktywację musi zawierać następujące informacje:

- Data złożenia wniosku o unieważnienie, zawieszenie lub reaktywację.
- Tożsamość użytkownika.
- Imię i nazwisko osoby wnioskującej o unieważnienie, zawieszenie lub reaktywację.
- Dane kontaktowe osoby wnoszącej o unieważnienie, zawieszenie lub reaktywację.
- Szczegółowy powód wniosku o unieważnienie

Żądanie musi zostać uwierzytelnione za pomocą EID, zgodnie z wymogami opisanymi w punkcie 3.4 niniejszej polityki, przed przystąpieniem do unieważnienia, zawieszenia lub ponownej aktywacji.

Usługę unieważnienia, zawieszenia lub reaktywacji można znaleźć na stronie internetowej EID pod adresem: https://www.electronicid.eu

W przypadku, gdy odbiorcą wniosku o unieważnienie, zawieszenie lub reaktywację przez osobę fizyczną wskazaną w certyfikacie jest podmiot użytkujący, po uwierzytelnieniu wniosku musi on wysłać w tym zakresie wniosek do EID.

Wniosek o unieważnienie, zawieszenie lub reaktywację zostanie rozpatrzony po jego otrzymaniu, a o zmianie statusu certyfikatu zostanie poinformowany użytkownik oraz ewentualnie osoba fizyczna wskazana w certyfikacie.

Tak samo usługa zarządzania unieważnieniem, zawieszeniem lub reaktywacją, jak i usługa konsultacji są uważane za usługi krytyczne i tym samym są uwzględnione w Planie Awaryjnym EID i Planie Ciągłości Działania.

4.1.14. Okres oczekiwania na wydanie wniosku o unieważnienie, zawieszenie lub reaktywację

Prośby o unieważnienie, zawieszenie lub reaktywację będą wysyłane natychmiast po otrzymaniu ich.

4.1.15. Okres oczekiwania na rozpatrzenie wniosku o cofnięcie, zawieszenie lub reaktywację.

Unieważnienie, zawieszenie lub reaktywacja nastąpi natychmiast po otrzymaniu

4.1.16. Obowiązek sprawdzania informacji o unieważnieniu lub zawieszeniu certyfikatów

Osoby trzecie muszą sprawdzić status tych certyfikatów, którym chcą zaufać.

Jedną z metod weryfikacji statusu certyfikatów jest zapoznanie się z najnowszą listą unieważnionych certyfikatów wydaną przez jednostkę certyfikującą EID.

Listy unieważnionych certyfikatów publikowane są w Repozytorium Jednostki Certyfikującej, a także pod następującymi adresami internetowymi, wskazanymi wewnątrz certyfikatów:

- http://crl1.uanataca.com/public/pki/crl/eid.crl
- http://crl2.uanataca.com/public/pki/crl/eid.crl

Status ważności certyfikatów można również sprawdzić za pomocą protokołu OCSP.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

4.1.17. Częstotliwość wydawania list unieważnionych certyfikatów (LRC)

EID wystawia LRC przynajmniej co 24 godziny.

LRC wskazuje planowany czas wystawienia nowego LRC, chociaż LRC może zostać wystawiony przed terminem wskazanym w poprzednim LRC, w celu przedstawienia odwołań.

LRC obowiązkowo przechowuje unieważniony lub zawieszony certyfikat do czasu jego wygaśnięcia.

4.1.18. Maksymalny termin publikacji LRC

LRC są publikowane w Repozytorium w rozsądnym terminie natychmiast po ich wygenerowaniu, który w żadnym wypadku nie przekracza kilku minut.

4.1.19. Dostępność usług sprawdzania online statusu certyfikatów

Aby sprawdzić ostatnią listę CRL wydaną w każdym CA, należy pobrać:

- *Główny urząd certyfikacji (UANATACA ROOT 2016):*

  - http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
  - http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

    - *Pośredni urząd certyfikacji 1 (EID CA1):*

  - http://crl1.uanataca.com/public/pki/crl/eid.crl
  - http://crl2.uanataca.com/public/pki/crl/eid.crl

W przypadku awarii systemów weryfikacji statusu certyfikatu z przyczyn niezależnych od EID, EID musi dołożyć wszelkich starań, aby usługa ta pozostawała nieaktywna przez jak najkrótszy okres, nieprzekraczający 24 godzin.

EID dostarcza osobom trzecim, które ufają certyfikatom, informacje o działaniu usługi informacji o stanie certyfikatów.

Jedną z metod weryfikacji statusu certyfikatów jest zapoznanie się z najnowszą listą unieważnionych certyfikatów wydaną przez jednostkę certyfikującą EID.

Listy unieważnionych certyfikatów publikowane są w Repozytorium Jednostki Certyfikującej, a także pod następującymi adresami internetowymi, wskazanymi wewnątrz certyfikatów:

- http://crl1.uanataca.com/public/pki/crl/eid.crl
- http://crl2.uanataca.com/public/pki/crl/eid.crl

Status ważności certyfikatów można również sprawdzić za pomocą protokołu OCSP.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

4.1.20. Obowiązek sprawdzania informacji o unieważnieniu lub zawieszaniu certyfikatów.

Obowiązkowe jest sprawdzenie statusu certyfikatów przed zaufaniem im.

Strony trzecie muszą zweryfikować status i ważność tych certyfikatów, którym chcą zaufać, mając możliwość użycia metody weryfikacji opisanej w poprzedniej sekcji (albo CRL lub OCSP).

4.1.21. Wymogi specjalne w przypadku świadczenia klucza prywatnego

O świadczeniu klucza prywatnego EID powiadamia wszystkich uczestników usług certyfikacyjnych, w miarę możliwości, publikując ten fakt na stronie internetowej EID, a także, jeśli uzna to za konieczne, w innych mediach, w tym listownie.

4.1.22. Maksymalny okres certyfikatu cyfrowego w stanie zawieszenia.

Maksymalny okres ważności certyfikatu cyfrowego w stanie zawieszonym jest nieograniczony do czasu jego wygaśnięcia.

4.1.23. Zakończenie użytkowania

Po upływie okresu ważności certyfikatu subskrypcja usługi zakończy się.

4.2. Certyfikaty długoterminowe

4.2.1. Wniosek o wydanie certyfikatu długoterminowego

4.2.1.1. Uprawnienie do wnioskowania o wydanie.

Ubiegający się o certyfikat musi podpisać z EID umowę o świadczenie usług certyfikacyjnych.

Równorzędnie, przed wydaniem i dostarczeniem certyfikatu, wniosek o wydanie certyfikatu musi znaleźć się w samej umowie, w określonym dokumencie formularza wniosku lub certyfikatu albo w urzędzie rejestracyjnym.

Jeżeli wnioskodawca jest osobą inną niż użytkownik, musi istnieć upoważnienie od użytkownika, aby wnioskodawca mógł złożyć wniosek, składając go na karcie wniosku o wydanie certyfikatu podpisanej przez wnioskodawcę we własnym imieniu dla certyfikatów osoby fizycznej.

4.2.2. Proces wniosku o certyfikację

4.2.2.1. Wykonywanie działań potrzebnych do identyfikacji i uwierzytelnienia

Po otrzymaniu wniosku o wydanie certyfikatu osoby fizycznej, EID zapewnia, że wnioski o wydanie certyfikatu są kompletne, dokładne i należycie autoryzowane przed ich przetworzeniem.

Jeśli wszystko jest poprawne, EID weryfikuje przekazane informacje, weryfikując aspekty opisane w punkcie 3.2.

W przypadku certyfikatu kwalifikowanego dokumentacja uzasadniająca przyznanie wniosku musi być przechowywana i należycie rejestrowana oraz z gwarancjami bezpieczeństwa oraz integralności przez okres 15 lat od wygaśnięcia ważności certyfikatu, nawet w przypadku wcześniejszej utraty ważności z powodu odwołania.

4.2.2.2. Zaakceptowanie lub odrzucenie wniosku

W przypadku poprawnej weryfikacji danych, EID musi zatwierdzić wniosek o wydanie zaświadczenia i przystąpić do jego wydania i dostarczenia.

Jeżeli weryfikacja wykaże, że informacje są nieprawidłowe lub istnieje podejrzenie, że są nieprawidłowe lub mogą mieć wpływ na reputację Urzędu Certyfikacji, Urzędów Rejestracji lub użytkowników, ELECTRONIC IDENTIFICATION, SL odrzuci wniosek, lub wstrzyma jego zatwierdzanie do czasu przeprowadzenia dodatkowych kontroli, które uzna należyte.

W sytuacji, gdy dodatkowe kontrole nie wykażą poprawności informacji, które mają zostać zweryfikowane, wniosek zostanie definitywnie odrzucony.

EID powiadamia wnioskodawcę o zatwierdzeniu lub odrzuceniu wniosku.

EID będzie mógł zautomatyzować procedury weryfikacji poprawności informacji, które będą zawarte w zaświadczeniach oraz akceptacji wniosków.

4.2.2.3. Okres rozstrzygnięcia wniosku

EID odpowiada na wnioski o wydanie certyfikatu w kolejności nadejścia, w rozsądnym terminie, a maksymalny okres gwarancji może być określony w umowie o wydanie certyfikatu.

Żądania pozostają aktywne, dopóki nie zostaną zatwierdzone lub odrzucone.

4.2.3. Wydanie certyfikatu

4.2.3.1. Działanie CA podczas procesu wydania

Po zatwierdzeniu wniosku o certyfikację certyfikat jest wydawany w sposób bezpieczny i udostępniany podpisującemu do akceptacji.

Procesy określone w tym rozdziale mają zastosowanie również w przypadku odnawiania certyfikatów, ponieważ powoduje to wydanie nowego certyfikatu.

Podczas procesu EID musi zająć się szeregiem zadań:

- Chroni poufność i integralność posiadanych danych rejestracyjnych.
- Korzysta z niezawodnych systemów i produktów, które są zabezpieczone przed wszelkimi zmianami i gwarantują bezpieczeństwo techniczne oraz w tym przypadku, kryptograficzne bezpieczeństwo obsługiwanych przez nie procesów certyfikacji.
- Generuje parę kluczy za pomocą procedury generowania certyfikatu, bezpiecznie połączonej z procedurą generowania kluczy.
- Wykorzystuje procedurę generowania certyfikatu, która bezpiecznie łączy certyfikat z informacjami rejestracyjnymi, w tym z certyfikowanym kluczem publicznym.
- Gwarantuje, że certyfikat jest wystawiany przez system stosujący zabezpieczenia przed fałszerstwem oraz gwarantujące poufność kluczy podczas procesu generowania ich.
- Wskazuje datę i godzinę wystawienia certyfikatu.
- Gwarantuje wyłączną kontrolę nad kluczami przez użytkownika, a sam EID ani jego Punkty Rejestracji nie mogą ich w żaden sposób wydedukować ani wykorzystać.

4.2.3.2. Powiadomienie użytkownika o wydaniu

EID informuje użytkownika i/lub osobę fizyczną wskazaną w certyfikacie o wydaniu certyfikatu oraz o sposobie generowania/pobierania.

4.2.4. Wydanie i zaakceptowanie certyfikatu

4.2.4.1. Odpowiedzialności CA

W trakcie tego procesu operator lub upoważniony personel Punktu Rejestracji musi wykonać następujące czynności:

- Udokumentować definitywnie tożsamość osoby fizycznej wskazanej w certyfikacie, zgodnie z postanowieniami tego dokumentu.
- Podpisać i zaakceptować przez użytkownika umowę o świadczeniu usług certyfikacyjnych drogą elektroniczną .
- Dostarczenie, w danych przypadkach, w zależności od rodzaju wydanego certyfikatu, arkusz dostarczenia i odbioru certyfikatu do osoby fizycznej wskazanej w certyfikacie, zawierający co najmniej poniżej wskazaną treść:
    - Podstawowe informacje dotyczące wykorzystania certyfikatu, w tym w szczególności informacje o dostawcy usług certyfikacyjnych oraz

obowiązujące oświadczenie dotyczące praktyk certyfikacyjnych, takie jak obowiązki, czynności i uprawnienia.

- Informacje o certyfikacie.
- Potwierdzenie przez osobę podpisującą otrzymania certyfikatu i/lub mechanizmów jego generowania/pobierania oraz akceptacji ww. elementów.
- System zobowiązań podpisującego.
- Odpowiedzialność podpisującego.
- Metoda przypisania wyłącznego klucza prywatnego i danych aktywacyjnych certyfikat.
- Data aktu dostawy i odbioru.

Wszystkie te informacje mogą być zawarte w samej umowie o świadczenie usług certyfikacyjnych. Reasumując, w momencie akceptacji Umowy o świadczenie usług certyfikacyjnych przez użytkownika, dostarczenie i odbiór certyfikatu będzie rozumiane jako zaakceptowanie certyfikatu.

- Uzyskać podpis osoby wskazanej w certyfikacie.

Za przeprowadzenie tych procesów odpowiedzialne są Punkty Rejestracji, które muszą dokumentować poprzednie czynności i przechowywać oryginały dokumentów (karty zdawczo-odbiorcze), przesyłać kopię elektroniczną do EID, a także oryginały, gdy EID żąda dostępu do nich.

4.2.4.2. Postępowanie stanowiące akceptację certyfikatu

Z chwilą doręczenia dokumentu odbioru, poświadczenie jest akceptowane przez osobę fizyczną wskazaną w certyfikacie poprzez podpisanie protokołu zdawczo-odbiorczego.

Kiedy wygenerowanie i dostarczenie certyfikatu następują jednocześnie według procedur określonych przez EID, akceptacja certyfikatu przez wskazaną w nim osobę fizyczną następuje poprzez podpisanie umowy o świadczenie usług certyfikacyjnych

4.2.4.3. Opublikowanie certyfikatów przez CA

Po wygenerowaniu certyfikatu przez Dostawcę Usług Certyfikacyjnych zostanie on opublikowany w katalogu, a konkretnie we wpisie odpowiadającym nazwie wyróżniającej

użytkownika, zgodnie z definicją zawartą w sekcji „Wydawanie certyfikatu" niniejszego załącznika.

Jeżeli wnioskodawca podał adres e-mail w procesie aplikacyjnym, zostanie mu wysłana informacja o dostępności Certyfikatu oraz możliwości korzystania.

4.2.4.4. Powiadomienie osób trzecich o wydaniu

EID nie powiadamia osób trzecich.

4.2.5. Używanie pary kluczy i certyfikatu

4.2.5.1. Używanie przez użytkownika

EID umownie zobowiązuje użytkownika do:

- Dostarczyć Urzędowi Certyfikacji pełne i adekwatne informacje, zgodnie z wymaganiami niniejszego Kodeksu Postępowania Certyfikacyjnego, w szczególności w odniesieniu do procedury rejestracji.
- Wyrazić swoją zgodę przed wydaniem i dostarczeniem certyfikatu.
- Bezzwłocznie zakomunikować do EID, Urzędów Rejestracji i każdej innej osobie, która według użytkownika może zaufać certyfikatowi:
  - o Utracie, kradzieży lub potencjalnej ingerencji w klucze prywatne. o Utracie kontroli nad kluczem prywatnym w wyniku ujawnienia danych aktywacyjnych (np. kodu PIN) lub z jakiegokolwiek innych powodów.
  - o Nieścisłości lub zmianach w treści certyfikatu, o których użytkownik wie lub może wiedzieć. o Utracie, zmianie, nieautoryzowanym użyciu, kradzieży lub naruszeniu karty, jeśli istnieje.
- Przekazać osobom fizycznym wskazanym w certyfikacie wypełnienie ich określonych obowiązków oraz ustanowić mechanizmy gwarantujące ich skuteczne wypełnianie.
- Nie należy monitorować, manipulować ani wykonywać czynności inżynierii wstecznej w zakresie technicznej realizacji usług certyfikacji EID bez uprzedniej pisemnej zgody.
- Użytkownik jako posiadacz certyfikatu, nie może przenieść jego użytkowania na osoby trzecie.
- Nie naruszać bezpieczeństwa usług certyfikacyjnych dostawcy usług certyfikacyjnych EID.

4.2.5.2. Użycie przez osoby trzecie, które ufają w certyfikaty.

EID informuje osobę trzecią, która ufa certyfikatom, że musi przyjąć następujące obowiązki:

- Doinformować się, czy certyfikat jest odpowiedni do zamierzonego zastosowania.
- Zweryfikować ważność, zawieszenie lub unieważnienie wydanych certyfikatów, do czego będzie wykorzystywał informacje o statusie certyfikatów.
- Zweryfikować wszystkie certyfikaty w hierarchii certyfikatów, zanim zaufa podpisowi cyfrowemu lub innemu z certyfikatów w hierarchii.
- Uznać, że zweryfikowane podpisy elektroniczne złożone w kwalifikowanym urządzeniu do tworzenia podpisów (DCCF) są prawnie uważane za kwalifikowane podpisy elektroniczne; czyli odpowiednik podpisów odręcznych, a także fakt, że certyfikat umożliwia tworzenie innych rodzajów podpisów elektronicznych i mechanizmów szyfrowania.
- Pamiętać o wszelkich ograniczeniach dotyczących korzystania z certyfikatu, niezależnie od tego, czy znajduje się ono w samym certyfikacie, czy w umowie strony trzeciej, która ufa certyfikatowi.
- Uwzględnić wszelkie środki ostrożności ustanowione w umowie lub innym instrumencie, niezależnie od ich charakteru prawnego.
- Nie monitorować, nie manipulować ani nie przeprowadzać czynności inżynierii wstecznej w zakresie technicznym realizacji usług certyfikacji EID bez uprzedniej pisemnej zgody.
- Nie narażać bezpieczeństwa usług certyfikacji EID.

4.2.6. Odnawianie kluczy i certyfikatów

Aktualne certyfikaty mogą być odnawiane poprzez określoną i uproszczoną procedurę składania wniosków, w celu zachowania ciągłości usługi certyfikacyjnej.

Odnowienie certyfikatów wymaga odnowienia kluczy, w sposób, opisany poniżej, aby zaobserwować przyczyny i procedurę odnawiania.

Użytkownicy mogą wnioskować o odnowienie Certyfikatów wydanych przez EID, pod warunkiem, że w chwili złożenia wniosku posiadają ważny certyfikat i powiązane z nim dane dotyczące tworzenia podpisu, a wniosek ten zostanie złożony w ciągu sześćdziesięciu (60) dni przed jego wygaśnięciem.

Wcześniejszy certyfikat, który został odnowiony, pozostanie ważny do wygaśnięcia. W przypadku żądania unieważnienia Certyfikatu, EID przystąpi do unieważnienia obu Certyfikatów.

Certyfikat zostanie uznany za zaakceptowany w momencie elektronicznego podpisania odnowienia.

EID publikuje odnowiony certyfikat w Repozytorium, o którym mowa w pkt 2.1., z zachowaniem odpowiednich zabezpieczeń.

Korzystanie z odnowionych Certyfikatów podlega tym samym ogólnym i szczegółowym warunkom obowiązującym w dowolnym czasie i ustalonym dla rodzaju odnawianego Certyfikatu.

4.2.7. Modyfikacja certyfikatów

Modyfikacja certyfikatów, z wyjątkiem modyfikacji certyfikowanego klucza publicznego, która jest uważana za odnowienie, będzie traktowana jako nowe wydanie certyfikatu, zgodnie z opisem w punktach 4.1, 4.2, 4.3 i 4.4.

4.2.8. Unieważnienie, zawieszenie lub reaktywacja certyfikatów

Unieważnienie certyfikatu zakłada definitywną utratę jego ważności i jest nieodwracalne.

Zawieszenie (lub czasowe unieważnienie) certyfikatu zakłada czasową utratę jego ważności i jest odwracalne. Wyłącznie certyfikaty podmiotu końcowego mogą podlegać zawieszeniu.

Reaktywacja certyfikatu oznacza jego przejście ze statusu zawieszonego do statusu aktywnego.

4.2.9. Powody unieważnienia certyfikatu

EID odmawia certyfikat, gdy wystąpi jedna z następujących przyczyn:

1) Okoliczności wpływające na informacje zawarte w certyfikacie:

a) Modyfikacja jakichkolwiek danych zawartych w certyfikacie, po odpowiednim wydaniu certyfikatu zawierającego modyfikacje.
b) Odkrycie, że pewne dane zawarte we wniosku certyfikatu są nieprawidłowe.
c) Odkrycie, że niektóre dane zawarte w certyfikacie są nieprawidłowe.

2) Okoliczności wpływające na bezpieczeństwo klucza lub certyfikatu:

a) Naruszenie klucza prywatnego, infrastruktury lub systemów dostawcy usług certyfikacyjnych, który wystawił certyfikat, o ile wpływa na wiarygodność certyfikatów wydanych w wyniku tego incydentu.
b) Naruszenie przez EID wymagań określonych w procedurach zarządzania certyfikatami, określonych w niniejszym Kodeksie Postępowania Certyfikacyjnego.
c) Naruszenie lub podejrzenie naruszenia bezpieczeństwa klucza lub wydanego certyfikatu.

d) Nieautoryzowany dostęp lub użycie przez stronę trzecią klucza prywatnego odpowiadającego kluczowi publicznemu zawartemu w certyfikacie.
e) Niepoprawne użycie certyfikatu przez wskazaną w certyfikacie osobę fizyczną lub brak sumienności w przechowywaniu klucza prywatnego.

3) Okoliczności mające wpływ na użytkownika lub wskazaną w certyfikacie osobę fizyczną:

a) Rozwiązanie stosunku prawnego o świadczenie usług pomiędzy EID a użytkownikiem.
b) Zmiana lub rozwiązanie istniejącego stosunku prawnego lub przyczyny, która spowodowała wydanie certyfikatu wskazanej w certyfikacie osobie fizycznej.
c) Naruszenie przez wnioskodawcę certyfikatu wcześniej ustalonych wymogów dla jego wniosku
d) Naruszenie przez użytkownika lub osobę wskazaną w certyfikacie ich zobowiązań, odpowiedzialności i gwarancji określonych w odpowiednim dokumencie prawnym.
e) Nagła niepełnosprawność lub śmierć posiadacza klucza.
f) Wniosek użytkownika o unieważnienie certyfikatu, zgodnie z postanowieniami pkt. 3.4.

4) Inne okoliczności

a) Zakończenie usługi certyfikacyjnej Urzędu Certyfikacji EID.
b) Używanie certyfikatu, które jest szkodliwe i jest kontynuowane dla EID. W takim sytuacji użycie go uważa się za szkodliwe względem następujących kryteriów:
    - Specyfika oraz ilość otrzymanych skarg.
    - Tożsamość podmiotów składających reklamacje
    - Odpowiednie przepisy obowiązujące w danym czasie.
    - Odpowiedź użytkownika lub osoby wskazanej w certyfikacie na otrzymane reklamacje.

4.2.9.1. Powody zawieszenia certyfikatu

Certyfikaty EID mogą zostać zawieszone z następujących powodów:

- Na żądanie użytkownika lub osoby fizycznej wskazanej w certyfikacie.
- Gdy dokumentacja wymagana we wniosku o unieważnienie jest wystarczająca, ale nie można dorzecznie zidentyfikować użytkownika lub osoby fizycznej wskazanej w certyfikacie.
- Brak używania certyfikatu przez długi czas, wcześniej znany.

- W przypadku podejrzenia o włamanie do klucza, do czasu jego potwierdzenia. W takim przypadku EID musi zadbać o to, aby certyfikat nie był zawieszony na dłużej niż jest to konieczne do potwierdzenia swojego zobowiązania.

4.2.9.2. Przyczyny reaktywacji certyfikatu

Świadectwa EID można reaktywować z następujących powodów:

- Gdy certyfikat jest w stanie zawieszenia.
- Na żądanie użytkownika lub osoby fizycznej wskazanej w certyfikacie.

4.2.9.3. Kto może ubiegać się o unieważnienie, zawieszenie lub reaktywacje

Mogą wystąpić o unieważnienie, zawieszenie lub reaktywację certyfikatu:

- Osoba wskazana w certyfikacie.
- Użytkownik certyfikatu za pośrednictwem podmiotu odpowiedzialnego za usługę certyfikacyjną.

4.2.9.4. Proces o unieważnienie, zawieszenie lub reaktywacje

Podmiot, który potrzebuje unieważnienia, zawieszenia lub reaktywacji certyfikatu, może zwrócić się o to bezpośrednio do EID lub Punktu Rejestracji użytkownika lub zrobić to samodzielnie za pośrednictwem serwisu internetowego dostępnego na stronie EID.

Wniosek o unieważnienie, zawieszenie lub reaktywację musi zawierać następujące informacje:

- Data złożenia wniosku o unieważnienie, zawieszenie lub reaktywację.
- Tożsamość użytkownika.
- Imię i nazwisko osoby wnioskującej o unieważnienie, zawieszenie lub reaktywację.
- Dane kontaktowe osoby wnoszącej o unieważnienie, zawieszenie lub reaktywację.
- Szczegółowy powód wniosku o unieważnienie

Żądanie musi zostać uwierzytelnione za pomocą EID, zgodnie z wymogami określonymi w punkcie 3.4 niniejszej polityki, przed przystąpieniem do unieważnienia, zawieszenia lub ponownej aktywacji.

W stosownych przypadkach usługę unieważnienia, zawieszenia lub reaktywacji można znaleźć na stronie internetowej EID pod adresem: https://www.electronicid.eu

W przypadku, gdy odbiorcą wniosku o unieważnienie, zawieszenie lub reaktywację przez osobę fizyczną wskazaną w certyfikacie jest podmiot użytkujący, po uwierzytelnieniu wniosku musi on wysłać w tym zakresie wniosek do EID.

Wniosek o unieważnienie, zawieszenie lub reaktywację zostanie rozpatrzony po jego otrzymaniu, a o zmianie statusu certyfikatu zostanie poinformowany użytkownik oraz ewentualnie osoba fizyczna wskazana w certyfikacie.

Zarówno usługa zarządzania unieważnieniem, zawieszeniem lub reaktywacją, jak i usługa konsultacji są uważane za usługi krytyczne i tym samym są uwzględnione w Planie Awaryjnym EID oraz Planie Ciągłości Działania.

4.2.9.5. Okres oczekiwania na wydanie wniosku o unieważnienie, zawieszenie lub reaktywację

Prośby o unieważnienie, zawieszenie lub reaktywację będą wysyłane natychmiast po otrzymaniu ich.

4.2.9.6. Okres oczekiwania na proces wniosku o unieważnienie zawieszenie lub reaktywacje

Unieważnienie, zawieszenie lub reaktywacja nastąpi niezwłocznie po jego otrzymaniu.

4.2.9.7. Obowiązek sprawdzania informacji o unieważnieniu lub zawieszeniu certyfikatów

Osoby trzecie muszą sprawdzić status certyfikatów, którym chcą zaufać.

Jedną z metod weryfikacji statusu certyfikatów jest zapoznanie się z najnowszą listą unieważnionych certyfikatów wydaną przez urząd certyfikacji EID.

Listy unieważnionych certyfikatów są publikowane w Repozytorium Urzędów Certyfikacji, a także pod następującymi adresami internetowymi, wskazanymi wewnątrz certyfikatów:

- http://crl1.uanataca.com/public/pki/crl/eid.crl
- http://crl2.uanataca.com/public/pki/crl/eid.crl

Status ważności certyfikatów można również sprawdzić za pomocą protokołu OCSP.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

4.2.9.8. Częstotliwość wydawania list unieważnionych certyfikatów (LRC)

EID wystawia LRC przynajmniej co 24 godziny.

LRC wskazuje planowany czas wystawienia nowego LRC, chociaż LRC może zostać wystawiony przed terminem wskazanym w poprzednim LRC, w celu przedstawienia odwołań.

LRC obowiązkowo przechowuje unieważniony lub zawieszony certyfikat do czasu jego wygaśnięcia.

4.2.9.9. Maksymalny termin publikacji LRCs

LRC są publikowane w Repozytorium w rozsądnym terminie natychmiast po ich wygenerowaniu, który w żadnym wypadku nie przekracza kilku minut.

4.2.9.10. Dostępność usług sprawdzania online statusu certyfikatów

Aby sprawdzić ostatnią listę CRL wydaną w każdym CA, należy pobrać:

- *Główny urząd certyfikacji (UANATACA ROOT 2016):*
  - http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
  - http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl
    - *Pośredni urząd certyfikacji 1 (EID CA1):*
  - http://crl1.uanataca.com/public/pki/crl/eid.crl
  - http://crl2.uanataca.com/public/pki/crl/eid.crl

W przypadku awarii systemów weryfikacji statusu certyfikatu z przyczyn niezależnych od EID, EID musi dołożyć wszelkich starań, aby usługa ta pozostawała nieaktywna przez jak najkrótszy okres, nieprzekraczający 24 godzin.

EID dostarcza osobom trzecim, które ufają certyfikatom, informacje o działaniu usługi informacji o stanie certyfikatów.

Jedną z metod weryfikacji statusu certyfikatów jest zapoznanie się z najnowszą listą unieważnionych certyfikatów wydaną przez urząd certyfikacji EID.

Listy unieważnionych certyfikatów są publikowane w Repozytorium Urzędów Certyfikacji, a także pod następującymi adresami internetowymi, wskazanymi wewnątrz certyfikatów:

- http://crl1.uanataca.com/public/pki/crl/eid.crl
- http://crl2.uanataca.com/public/pki/crl/eid.crl

Status ważności certyfikatów można również sprawdzić za pomocą protokołu OCSP.

http://ocsp1.uanataca.com/public/pki/ocsp/

http://ocsp2.uanataca.com/public/pki/ocsp/

4.2.9.11. Obowiązek dowiadywania się o usługi sprawdzania statusu certyfikatu

Obowiązkowe jest sprawdzenie statusu certyfikatów przed zaufaniem im.

Strony trzecie muszą zweryfikować status i ważność tych certyfikatów, którym chcą zaufać, mając możliwość użycia metody weryfikacji opisanej w poprzedniej sekcji (albo CRL lub OCSP).

4.2.9.12. Wymogi specjalne w przypadku świadczenia klucza prywatnego

O świadczeniu klucza prywatnego EID powiadamia się wszystkich uczestników usług certyfikacyjnych, w miarę możliwości, publikując ten fakt na stronie internetowej EID, a także, jeśli uzna to za konieczne, w innych mediach, w tym papierowych.

4.2.9.13. Maksymalny okres certyfikatu cyfrowego w stanie zawieszenia

Maksymalny okres ważności certyfikatu cyfrowego w stanie zawieszonym jest nieograniczony do czasu jego wygaśnięcia.

4.2.10. Zakończenie użytkowania

Po upływie okresu ważności certyfikatu użytkownika usługi zakończy się.

W drodze wyjątku użytkownik może utrzymywać dotychczasową usługę, wnosząc o odnowienie certyfikatu, z zastrzeżeniem określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego.

EID może wydać nowy certyfikat z urzędu, o ile użytkownicy utrzymują ten status.

4.2.11. Depozyt i odzyskiwanie kluczy

4.2.11.1. Polityka i praktyki dotyczące depozytów i odzyskiwania kluczy

EID nie świadczy usług depozytu i odzyskiwania kluczy.

4.2.11.2. Polityka i zasady szyfrowania oraz restaurowania kluczy sesji

Bez zastrzeżeń.

5. Bezpieczeństwo fizyczne, kontrola zarządzania i operacji

5.1. Infrastruktura i sprzęt obsługujący usługę Identyfikacji Wideo.

Infrastruktura i sprzęt wspierający usługę wideo identyfikacji znajdują się w chronionych pomieszczeniach o ograniczonym dostępie, ponieważ dostęp do nich możliwy jest tylko przez zaplanowane i monitorowane wejścia, a cały personel wchodzący do tych pomieszczeń zostanie zidentyfikowany, rejestrując wejścia i wyjścia. EID gwarantuje spełnienie wymagań określonych w rozdziale V Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.

W przypadku korzystania z usług zewnętrznych dostawców infrastruktury upoważnieni będą tylko ci, którzy przestrzegają tych kontroli.

5.2. Fizyczne kontrole bezpieczeństwa

EID za pośrednictwem infrastruktury klucza publicznego UANATACA, S.A. świadczy swoje usługi certyfikacyjne, które ustanowiły fizyczne i środowiskowe środki kontroli w celu ochrony zasobów obiektów, w których znajdują się systemy, samych systemów oraz sprzętu wykorzystywanego do operacji świadczenia zaufanych usług elektronicznych.

Szczególnie polityka bezpieczeństwa mająca zastosowanie do elektronicznych usług zaufania określa zalecenia dotyczące następujących kwestii:

- Fizyczne kontrole dostępu.
- Ochrona przed klęskami żywiołowymi.
- Środki ochrony przeciwpożarowej.
- Awaria systemów wsparcia (elektronika, telekomunikacja itp.)
- Zawalenie się konstrukcji.
- Powodzie.
- Ochrona przed kradzieżą.
- Nieautoryzowane wyniesienie sprzętu, informacji, wsparć i aplikacji związanych z komponentami wykorzystywanymi do usług dostawcy usług certyfikacyjnych.

Środki te mają zastosowanie do obiektów, z których świadczone są elektroniczne usługi zaufania, w ich środowiskach produkcyjnych i awaryjnych, które podlegają okresowym audytom zgodnie z obowiązującymi przepisami i przewidzianymi w tym celu politykami.

Obiekty posiadają systemy konserwacji zapobiegawczej i naprawczej ze wsparciem 24 godziny na dobę, 365 dni w roku ze wsparciem w ciągu 24 godzin od zgłoszenia.

5.2.1. Lokalizacja i budowa obiektów

Ochronę fizyczną osiąga się poprzez stworzenie jasno określonych granic bezpieczeństwa wokół usług. Jakość i solidność materiałów konstrukcyjnych obiektów gwarantuje odpowiedni poziom ochrony przed włamaniami oraz znajduje się w obszarze o niskim ryzyku katastrof oraz umożliwia szybki dostęp.

Pomieszczenie, w którym wykonywane są operacje kryptograficzne w Centrum Przetwarzania Danych posiada redundancję w swojej infrastrukturze, a także kilka alternatywnych źródeł energii elektrycznej i chłodzenia na wypadek sytuacji awaryjnych.

Dostępne są udogodnienia, które fizycznie chronią świadczenie usług zatwierdzania żądań certyfikatów i zarządzania ich odwołaniami przed nieautoryzowanym dostępem do systemów lub danych, a także ich ujawnieniem.

5.2.2. Fizyczny dostęp

Istnieją trzy poziomy bezpieczeństwa fizycznego (wejście do budynku, w którym znajduje się CPD, dostęp do pomieszczenia CPD oraz dostęp do Rack) dla ochrony usługi generowania certyfikatów i muszą być dostępne z poziomów niższych na wyższe.

Dostęp do obiektów, w których przeprowadzane są procesy certyfikacji, jest ograniczony i chroniony poprzez połączenie środków fizycznych i proceduralnych. W ten sposób:

- Ogranicza się do wyraźnie upoważnionego personelu, z identyfikacją w momencie dostępu i rejestracji, w tym filmowania przez telewizję przemysłową i jej archiwum.
- Dostęp do pomieszczeń odbywa się poprzez czytniki kart identyfikacyjnych zarządzany jest przez system informatyczny, który prowadzi dziennik wejść i wyjść.
- Aby uzyskać dostęp do pomieszczenia, w którym znajdują się procesy kryptograficzne, potrzebna jest uprzednia autoryzacja od administratorów usług hostingowych, którzy mają klucz do otwarcia klatki.

5.2.3. Elektryka i klimatyzacja

Obiekty wyposażone są w urządzenia stabilizujące prąd oraz system zasilania elektrycznego urządzeń duplikowanych z agregatem prądotwórczym.

Pomieszczenia, w których znajduje się sprzęt komputerowy, wyposażone są w systemy kontroli temperatury wraz z urządzeniami klimatyzacyjnymi.

5.2.4. Ekspozycja na wodę

Obiekty znajdują się w strefie niskiego ryzyka powodziowego.

Pomieszczenia, w których znajduje się sprzęt komputerowy, posiadają system wykrywania

wilgoci.

5.2.5. Zapobieganie i ochrona przeciwpożarowa

Obiekty i aktywa wyposażone są w automatyczne systemy wykrywania i gaszenia pożaru.

5.2.6. Przechowywanie multimediów

Tylko upoważniony personel ma dostęp do nośników pamięci.

Informacje klasyfikacyjne najwyższego poziomu są przechowywane w skrytce depozytowej poza obiektami Centrum Przetwarzania Danych.

5.2.7. Utylizacja odpadów

Usuwanie nośników, zarówno papierowych, jak i magnetycznych, odbywa się poprzez mechanizmy gwarantujące brak możliwości odzyskania informacji.

W przypadku nośników magnetycznych są wyrzucane, w takim przypadku są fizycznie niszczone lub są ponownie wykorzystywane po trwałym usunięciu lub procesie formatowania. W przypadku dokumentacji papierowej, za pomocą niszczarek lub w specjalnie przystosowanych do tego pojemnikach do późniejszego zniszczenia kontrolowanego.

5.2.8. Kopia zapasowa poza siedzibą

Bezpieczny magazyn zewnętrzny służy do przechowywania dokumentów, urządzeń magnetycznych i elektronicznych, które są niezależne od centrum operacyjnego.

5.3. Kontrole proceduralne

EID gwarantuje, że jej systemy działają w sposób bezpieczny, z tego powodu ustanowiła i wdrążyła procedury dotyczące funkcji mających wpływ na świadczenie jej usług.

Personel służby EID przeprowadza procedury administracyjne i zarządcze zgodnie z polityką bezpieczeństwa.

5.3.1. Funkcje bezpieczeństwa

Zgodnie z polityką bezpieczeństwa następujące funkcje zostały uznane za godne zaufania:

- **Audytor wewnętrzny:** Jest odpowiedzialny za przestrzeganie procedur operacyjnych. Jest to osoba spoza działu systemów informatycznych. Zadania Audytora Wewnętrznego są nieprzystające w czasie z zadaniami Certyfikacji i niezgodne z Systemami. Funkcje te będą podporządkowane szefowi operacji, podlegającemu zarówno jemu, jak i kierownictwu technicznemu.
- **Administrator systemów:** Odpowiedzialny za prawidłowe działanie hardware

oraz wsparcie programowe platformy certyfikacyjnej.

- **Administrator CA:** Odpowiada za czynności, które mają być wykonane na materiale kryptograficznym lub za wykonanie jakiejkolwiek funkcji, która wiąże za sobą aktywację kluczy prywatnych urzędów certyfikacji opisanych w niniejszym dokumencie lub któregokolwiek z jego elementów.
- **Operator CA:** Niezbędny odpowiedzialny wspólnie z Administratorem CA za opiekę nad materiałem aktywacyjnym kluczy kryptograficznych, odpowiedzialny również za operacje tworzenia kopii zapasowych i utrzymanie CA.
- **Operator Rejestru:** Osoba odpowiedzialna za zatwierdzanie wniosków certyfikacyjnych składanych przez subskrybenta oraz wydawanie certyfikatów cyfrowych.
- **Specjalista od Unieważnień:** Osoba odpowiedzialna za dokonywanie zmian w statusie certyfikatu, głównie za dokonywanie jego zawieszania i unieważniania.
- **Kierownik Bezpieczeństwa:** Odpowiedzialny za koordynację, kontrolę i zapewnienie środków bezpieczeństwa określonych w politykach bezpieczeństwa. Musi odpowiadać za aspekty związane z bezpieczeństwem informacji: logiczne, fizyczne, sieciowe, organizacyjne itp.

Osoby zajmujące powyższe stanowiska podlegają określonym procedurom śledczym i kontrolnym. Dodatkowo wdrażane są kryteria i procedury rozdziału funkcji, jako środek zapobiegający nieuczciwym działaniom.

5.3.2. Liczba osób na zadanie

Gwarantowane są co najmniej dwie osoby do wykonywania zadań związanych z generowaniem, odtwarzaniem i wykonywaniem kopii zapasowej klucza prywatnego Urzędów Certyfikacji. To samo kryterium stosuje się do realizacji zadań wydawania i aktywacji certyfikatów i kluczy prywatnych Urzędów Certyfikacji oraz ogólnie do wszelkich manipulacji urządzeniem do przechowywania kluczy głównego i pośredniego Urzędu Certyfikacji.

5.3.3. Identyfikacja i uwierzytelnianie dla każdej roli

Osoby przypisane do poszczególnych ról są identyfikowane przez audytora wewnętrznego, który czuwa nad tym, aby każda osoba wykonywała czynności, do których została przypisana.

Każda osoba kontroluje tylko zasoby niezbędne do jej roli, zapewniając w ten sposób, że żadna osoba nie ma dostępu do nieprzydzielonych zasobów.

Dostęp do zasobów odbywa się w zależności od aktywów za pomocą nazwy użytkownika/hasła, certyfikatu cyfrowego, fizycznej karty dostępu i/lub kluczy.

5.3.4. Role wymagające rozdzielenia obowiązków

Poniższe zadania wykonują co najmniej dwie osoby:

- Zadania pełnione przez Audytora będą niekompatybilne z obsługą i administracją systemów oraz w ogólności tych dedykowanych bezpośredniemu świadczeniu elektronicznych usług zaufania.
- Wydawanie i unieważnianie certyfikatów będą zadaniami niezgodnymi z Administracją i obsługą systemów.
- Administracją i eksploatacją systemów oraz jeśli CA są ze sobą niezgodne.

5.3.5. System zarządzania PKI

System PKI składa się z następujących modułów:

- Moduł Urzędu Certyfikacji. Urząd certyfikacji został zaprojektowany jako rozwiązanie dwuwarstwowe składające się z głównego urzędu certyfikacji i co najmniej jednego podrzędnego urzędu certyfikacji (w dalszej części podrzędnego urzędu certyfikacji). Root CA wydaje certyfikaty dla Sub CA, podczas gdy Sub CA wystawia certyfikaty dla podmiotów końcowych, takich jak usługi, firmy, użytkownicy lub usługi znakowania czasem.
- Moduł Urzędu Rejestracji. RA to aplikacja do zarządzania cyklem życia certyfikatu. Aplikacja ta umożliwia operatorowi zarządzanie całym cyklem życia certyfikatu.
- Moduł Uprawnienia co Weryfikacji. Autorytet Weryfikacji to aplikacja udostępniająca usługę weryfikacji certyfikatów online OCSP.
- Moduł zarządzania żądaniami. Usługa odpowiedzialna za przetwarzanie i przekierowywanie wszystkich żądań i żądań związanych ze świadczeniem Usług Zaufania wraz z pozostałymi elementami funkcjonalnymi składającymi się na Infrastrukturę Klucza Publicznego.
- Moduł zarządzania kluczami (HSM). HSM jest elementem odpowiedzialnym za przechowywanie klucza głównego używanego do zarządzania wszystkimi parami kluczy utworzonymi przez system. Wykonuje również operacje kryptograficzne z tymi kluczami.
- Moduł bazy danych. Komponent odpowiedzialny za Bazę Danych zbiera i przechowuje wszystkie informacje dostarczane przez kompletną infrastrukturę.

5.4. Kontrola personelu

5.4.1. Historia, kwalifikacje, doświadczenie i wymagania dotyczące uprawnień

Cały personel jest wykwalifikowany i/lub został odpowiednio poinstruowany do wykonywania przydzielonych mu operacji.

Pracownicy na stanowiskach zaufania nie mają interesów osobistych, które stoją w sprzeczności z wykonywaniem powierzonej im funkcji.

EID zapewnia, że personel rejestracyjny jest niezawodny w wykonywaniu zadań rejestracyjnych. Administrator Rejestru przechodzi szkolenie w zakresie wykonywania zadań weryfikacji wniosków.

Reasumując, pracownik zostanie zwolniony z obowiązków zaufania, gdy będzie miał wiedzę o istnieniu konfliktu interesów i/lub popełnieniu czynu karalnego, który może mieć wpływ na wykonywanie jego zadań.

Nie przypisze się niegodnej zaufania osoby, która nie nadaje się na stanowisko, zwłaszcza ze względu ryzyka, która może ponieść działalność. Z tego powodu,

Wcześniej przeprowadza się dochodzenie w zakresie dozwolonym przez obowiązujące prawo, dotyczące następujących aspektów:

- Studia, w tym deklarowany stopień naukowy.
- Poprzednie prace, do pięciu lat, w tym referencje zawodowe.
- Profesjonalne referencje.

W każdym przypadku Punkty Rejestracji mogą ustanowić różne procesy sprawdzania przeszłości, zawsze zachowując zasady EID, ponosząc odpowiedzialność za działania osób, które upoważniają do prowadzenia działalności.

5.4.2. Procedury dochodzenia historii

Przed zatrudnieniem osoby lub udostępnieniem jej do pracy przeprowadza się następujące kontrole:

- Referencje prac z ostatnich lat
- Profesjonalne referencje
- Studia, w tym deklarowany stopień naukowy.

EID uzyskuje jednoznaczną zgodę zainteresowanej strony na wspomniane wcześniejsze dochodzenie oraz przetwarza i chroni wszystkie jej dane osobowe zgodnie z obowiązującymi przepisami o ochronie danych osobowych, odzwierciedlonymi w europejskim rozporządzeniu nr 2016/679 Ogólne o ochronie danych i ogólnie wszelkie obowiązujące przepisy krajowe.

Wszelkie kontrole przeprowadzane są w zakresie dozwolonym przez obowiązujące prawo. Przyczyny, które mogą doprowadzić do odrzucenia kandydata na wiarygodne stanowisko, są następujące:

- Fałszerstwa w podaniu o pracę sporządzonym przez kandydata.
- Bardzo negatywne lub bardzo nierzetelne referencje zawodowe w związku z kandydatem.

5.4.3. Wymagania szkoleniowe

EID szkoli pracowników do stanowisk rzetelnych i kierowniczych, do czasu uzyskania niezbędnych kwalifikacji, prowadząc ewidencję tych szkoleń.

Programy szkoleniowe są okresowo przeglądane i aktualizowane, aby uzyskać najlepsze rezultaty.

Szkolenie obejmuje co najmniej następującą tematykę:

- Zasady i mechanizmy bezpieczeństwa hierarchii certyfikacji oraz środowiska użytkownika osoby szkolonej.
- Zadania do wykonania przez pracownika.
- Polityki i procedury bezpieczeństwa. Użytkowanie i obsługa zainstalowanych maszyn i aplikacji.
- Zarządzanie i przetwarzanie incydentów oraz zobowiązań w zakresie bezpieczeństwa.
- Ciągłość działania i procedury awaryjne.
- Procedura zarządzania i bezpieczeństwa w związku z przetwarzaniem danych osobowych.

EID gwarantuje, że weryfikacja dokumentów oraz weryfikacja tożsamości dokonywana jest przez odpowiednio przeszkolony personel.

5.4.4. Wymagania i częstotliwość odnawiania szkolenia

EID odnawia szkolenia personelu w razie potrzeby, a często na tyle, aby wykonywać swoje obowiązki kompetentnie i satysfakcjonująco, zwłaszcza gdy wprowadzane są istotne zmiany w zadaniach certyfikacyjnych.

5.4.5. Kolejność i częstotliwość rotacji stanowisk

Nie dotyczy.

5.4.6. Kary za nieuprawnione działania

EID posiada system sankcji, mający na celu usunięcie odpowiedzialności wynikającej z nieuprawnionych działań, dostosowany do obowiązującego prawa pracy.

Działania dyscyplinarne obejmują zawieszenie, oddzielenie od obowiązków, a nawet zwolnienie osoby odpowiedzialnej za szkodliwe działanie, proporcjonalnie do powagi niedozwolonego działania.

5.4.7. Profesjonalne wymagania dotyczące zatrudniania

Pracownicy zatrudnieni do wykonywania rzetelnych zadań podpisują z wyprzedzeniem klauzule poufności i wymogi operacyjne stosowane przez EID. Wszelkie działania zagrażające bezpieczeństwu przyjętych procesów mogą po oszacowaniu wykroczenia doprowadzić do rozwiązania umowy o pracę.

W przypadku, gdy całość lub część usług certyfikacyjnych jest obsługiwana przez stronę trzecią, kontrole i postanowienia zawarte w niniejszym rozdziale lub w innych częściach Kodeksu Postępowania Certyfikacyjnego będą stosowane i przestrzegane przez stronę trzecią, która wykonuje Funkcje

dogodności usług certyfikacyjnych, niezależnie od tego, czy podmiot certyfikujący będzie w każdym przypadku odpowiedzialny za skuteczne wykonanie. Aspekty te określone są w akcie prawnym służącym do uzgadniania świadczenia usług certyfikacyjnych przez podmiot trzeci inny niż EID.

5.4.8. Dostarczenie dokumentacji personelowi

Dostawca usług certyfikacyjnych będzie przez cały czas dostarczać dokumentację ściśle wymaganą przez swoich pracowników, aby wykonywać swoją pracę w sposób kompetentny i zadowalający.

5.5. Procedury audytu bezpieczeństwa

5.5.1. Typy wydarzeń rejestrowanych

Zachodzą i są rejestrowane co najmniej zdarzenia związane z bezpieczeństwem podmiotu:

- Włączanie i wyłączanie systemu.
- Próby tworzenia, usuwania, ustawiania haseł lub zmiany uprawnień.
- Próby logowania i wylogowania.
- Nieautoryzowane próby dostępu do systemu klimatyzacji przez sieć.
- Nieautoryzowane próby dostępu do systemu plików.
- Fizyczny dostęp do logów.
- Zmiany w konfiguracji i utrzymaniu systemu.
- Ewidencja wniosków CA.
- Włączanie i wyłączanie aplikacji AC.
- Zmiany w szczegółach urzędu certyfikacji i/lub jego kluczy.
- Zmiany w tworzeniu polityk certyfikatów.
- Generowanie własnych kluczy.
- Tworzenie i unieważnianie certyfikatów.
- Ewidencja zniszczenia nośnika zawierającego klucze, dane aktywacyjne.
- Zdarzenia związane z cyklem życia modułu kryptograficznego, takie jak jego odbiór, użytkowanie i dezinstalacja.
- Ceremonia wygenerowania kluczy i bazy danych zarządzania kluczami.
- Dzienniki dostępu fizycznego.
- Utrzymanie i zmiany konfiguracji systemu.
- Zmiany personalne.
- Raporty o zobowiązaniach i rozbieżnościach.
- Zapisy zniszczenia materiału zawierającego kluczowe informacje, dane aktywacyjne lub dane osobowe subskrybenta, w przypadku certyfikatów osób fizycznych lub osoby fizycznej wskazanej w certyfikacie, w przypadku certyfikatów organizacji.

- Posiadanie danych aktywacyjnych dla operacji z kluczem prywatnym Urzędu Certyfikacji.
- Pełne raporty prób fizycznych włamań do infrastruktur obsługujących wydawanie certyfikatów i zarządzanie nimi.

Wpisy rejestru obejmują następujące elementy:

- Data i godzina wejścia.
- Numer seryjny lub sekwencja wpisu w zapisach automatycznych.
- Tożsamość podmiotu wpisywanego do rejestru.
- Typ pozwolenia wejścia.

5.5.2. Częstotliwość przetwarzania rejestru kontroli

Rejestry są przeglądane po wystąpieniu alertu systemowego z powodu nastąpienia incydentu.

Przetwarzanie rejestrów kontroli obejmuje przegląd rejestrów, który obejmuje weryfikację, czy nie zostały one naruszone, krótką inspekcję wszystkich wpisów w dzienniku oraz dalsze badanie wszelkich alertów lub nieprawidłowości w rejestrach. Działania podjęte podczas przeglądu audytu są dokumentowane.

Utrzymywany system pozwala zagwarantować:

- Wystarczającą ilość miejsca do przechowywania logs.
- Pliki rejestru nie są przepisywane.
- Zapisywane informacje obejmują co najmniej: typ zdarzenia, datę i godzinę, użytkownika, który wykonuje wydarzenie oraz wynik operacji.
- Pliki dziennika zostaną zapisane w uporządkowanych plikach, które można włączyć do bazy danych w celu późniejszej eksploracji.

5.5.3. Okres przechowywania rejestru audytu

Informacje w logach są przechowywane przez okres od 1 do 15 lat, w zależności od rodzaju zarejestrowanych informacji.

5.5.4. Ochrona rejestru kontroli

Dzienniki systemowe:

- Są chronione przed manipulacją poprzez podpisanie plików, które je zawierają.
- Przechowywane są w urządzeniach ognioodpornych.

- Dostępność do niej jest chroniona przez przechowywanie w obiektach poza ośrodkiem, w którym znajduje się CA.

Dostęp do plików logów jest zarezerwowany tylko dla upoważnionych osób. Podobnie urządzenia są przez cały czas obsługiwane przez upoważniony personel.

Istnieje procedura wewnętrzna szczegółowo opisująca procesy zarządzania urządzeniami zawierającymi dane dziennika audytu.

5.5.5. Procedury tworzenia kopii zapasowej

Istnieje odpowiednia procedura tworzenia kopii zapasowych, aby w przypadku utraty lub zniszczenia ważnych plików odpowiednie kopie zapasowe rejestrów były dostępne w krótkim czasie (backup logs).

Wprowadzono procedurę bezpiecznego tworzenia kopii zapasowych rejestrów audytu, co tydzień wykonując kopię wszystkich rejestrów na nośniku zewnętrznym. Dodatkowo kopia jest przechowywana w zewnętrznej bazie.

5.5.6. Lokalizacja systemu zbioru rejestru audytów

Informacje dotyczące audytu zdarzeń są gromadzone wewnętrznie i automatycznie przez system operacyjny, komunikację sieciową i oprogramowanie do zarządzania certyfikatami, oprócz ręcznie generowanych danych, które będą przechowywane przez należycie upoważniony personel. Wszystko to składa się na system gromadzenia zapisów audytowych.

5.5.7. Powiadomienie o wydarzeniu audytu do podmiotu wydarzenia

Gdy system gromadzenia rejestrów audytu rejestruje zdarzenie, nie ma potrzeby wysyłania powiadomienia do osoby, organizacji, urządzenia lub aplikacji, która spowodowała zdarzenie.

5.5.8. Analiza słabych punktów

Analiza podatności za zagrożenia jest objęta procesami audytu infrastruktury klucza publicznego.

Skanowania w poszukiwaniu luk powinny być uruchamiane, przeglądane i poprawiane poprzez zbadanie monitorowanych zdarzeń. Analizy te muszą być przeprowadzane okresowo zgodnie z przewidzianą w tym celu wewnętrzną procedurą.

Dane audytu systemów są przechowywane w celu wykorzystania ich w badaniu każdego incydentu oraz w celu zlokalizowania luk w zabezpieczeniach.

5.6. Pliki informacyjne

Gwarantujemy, że wszystkie informacje związane z certyfikatami są przechowywane przez pewien okres w odpowiednim czasie, jak określono w punkcie 5.5.2 niniejszej polityki.

5.6.1. Rodzaje akt archiwalnych

Następujące dokumenty biorące udział w cyklu życia certyfikatu są przechowywane przez EID (lub przez podmioty rejestrujące):

- Wszystkie dane audytu systemu.
- Wszystkie dane związane z certyfikatami, w tym umowy z podpisującymi oraz dane związane z ich identyfikacją i lokalizacją
- Wnioski o wydanie i unieważnienie certyfikatów.
- Rodzaj dokumentu przedstawionego we wniosku o wydanie certyfikatu.
- Tożsamość jednostki rejestracyjnej, która akceptuje żądanie certyfikatu.
- Niepowtarzalny numer identyfikacyjny podany w poprzednim dokumencie.
- Wszystkie certyfikaty wydane lub opublikowane.
- Wydane listy CRL lub ewidencja statusu wygenerowanych certyfikatów.
- Historia wygenerowanych kluczy.
- Komunikacja między elementami PKI.
- Zasady i praktyki certyfikacji
- Wszystkie dane audytu zidentyfikowane w sekcji 5.4
- Informacje o wnioskach certyfikacyjnych.
- Dostarczona dokumentacja uzasadniająca wnioski certyfikacyjne.
- Informacje o cyklu życia certyfikatu.

EID i/lub odpowiednie urzędy rejestracji będą odpowiedzialne za prawidłowe złożenie wszystkich dokumentów.

5.6.2. Okres przechowywania rejestrów

Powyższe zapisy są archiwizowane przez co najmniej 15 lat lub okres ustalony przez obowiązujące przepisy.

W szczególności ewidencja unieważnionych certyfikatów dostępna na Listach unieważnionych certyfikatów oraz za pośrednictwem usługi weryfikacji statusu certyfikatu online (OCSP), będzie dostępna do bezpłatnego wglądu przez co najmniej 15 lat od daty wydania lub przez okres ustalony od jego zmiany statusu.

5.6.3. Ochrona plików

Plik jest chroniony, dostęp do niego mają tylko należycie upoważnione osoby. Plik jest chroniony przed przeglądaniem, modyfikacją, usunięciem lub jakąkolwiek inną manipulacją poprzez przechowywanie go w zaufanym systemie.

Właściwą ochronę plików zapewnia dysponowanie wykwalifikowanym personelem do obróbki i przechowywania w bezpiecznych obiektach poza zakładem.

5.6.4. Procedury tworzenia kopii zapasowej

Dostępne jest zewnętrzne centrum przechowywania gwarantujące dostępność kopii elektronicznego archiwum plików. Fizyczne dokumenty są przechowywane w bezpiecznych miejscach, gdzie dostęp mają tylko upoważnieni pracownicy

Co najmniej codziennie tworzone są przyrostowe kopie zapasowe wszystkich dokumentów elektronicznych, a pełne kopie zapasowe są tworzone co tydzień w razie odzyskiwania danych.

Ponadto EID (lub organizacje pełniące funkcję rejestracyjną) przechowują kopię dokumentów papierowych w bezpiecznym miejscu innym niż pomieszczenia samej Jednostki Certyfikującej.

5.6.5. Wymagania dotyczące wyznacznika daty i godziny

Zapisy są datowane z wiarygodnego źródła za pośrednictwem NTP.

Nie ma potrzeby podpisywania cyfrowo tych informacji.

5.6.6. Lokalizacja systemu plików

Istnieje scentralizowany system zbierania informacji o działalności zespołów zaangażowanych w usługę zarządzania certyfikatami.

5.6.7. Procedury uzyskiwania i weryfikowania informacji o plikach

Istnieje procedura opisująca proces weryfikacji, czy podane informacje są prawidłowe i dostępne. Informacje i środki weryfikacji są przekazywane audytorowi.

5.7. Odnawianie kluczy

Przed wygaśnięciem klucza prywatnego urzędu certyfikacji zostanie wykonana zmiana klucza. Stary urząd certyfikacji i jego klucz prywatny będą używane tylko do podpisywania list CRL, o ile istnieją aktywne certyfikaty wydane przez ten urząd certyfikacji. Nowy AC (Urząd Certyfikacji) zostanie wygenerowany z nowym kluczem prywatnym i nową nazwą wyróżniającą. Zmiana kluczy abonenckich odbywa się poprzez przeprowadzenie nowego procesu wydawania.

Ewentualnie, w przypadku podległych Urzędów Certyfikacji, można wybrać odnowienie certyfikatu ze zmianą kluczy lub bez, przy czym procedura opisana powyżej nie ma zastosowania.

5.8. Kompromis i odzyskiwanie po awarii

5.8.1. Procedury zarządzania incydentami i odstępstwami

EID opracowało polityki bezpieczeństwa i ciągłości działania, które pozwalają na zarządzanie i odzyskiwanie systemów w przypadku wystąpienia incydentów i naruszeń jej działania, zapewniając krytyczne usługi unieważniania i publikacji statusu certyfikatów.

5.8.2. Uszkodzenie zasobów, aplikacji i danych

W przypadku wystąpienia uszkodzenia zasobów, aplikacji lub danych, będą przestrzegane odpowiednie procedury zarządzania zgodnie z zasadami bezpieczeństwa i zarządzania incydentami EID, które obejmują wzmożenie, dochodzenie i reagowanie na incydent. W razie potrzeby zostaną rozpoczęte procedury odstąpienia klucza lub odzyskiwania po awarii.

5.8.3. Odstępstwo klucza prywatnego jednostki

W przypadku podejrzenia lub wiedzy o włamaniu zostaną uruchomione kluczowe procedury włamania zgodnie z politykami bezpieczeństwa, zarządzania incydentami i ciągłości działania, co pozwoli na przywrócenie krytycznych systemów, w razie potrzeby w centrum danych.

5.8.4. Kontynuacja współpracy po awarii

EID przywróci usługi krytyczne (zawieszanie i unieważnianie oraz publikacja informacji o statusie certyfikatu) zgodnie z istniejącym planem incydentów i ciągłości działania, przywracając normalne działanie powyższych usług w ciągu 24 godzin od awarii.

EID posiada alternatywne centrum, jeśli jest to konieczne do wdrożenia systemów certyfikacji opisanych w planie ciągłości działania.

5.9. Zakończenie usług

EID zapewnia, że ewentualne przerwy dla użytkowników i osób trzecich są minimalne w wyniku zakończenia świadczenia usług dostawcy usług certyfikacyjnych. W tym

przypadku gwarantowane jest ciągłe utrzymywanie zapisów określonych w sekcji 5.5.1 przez czas określony w sekcji 5.5.2 niniejszego Kodeksu Postępowania Certyfikacyjnego.

Niezależnie od powyższego, jeśli jest to konieczne EID wykona wszelkie czynności niezbędne do przeniesienia na osobę trzecią lub do depozytu notarialnego obowiązków utrzymywania określonych zapisów w odpowiednim okresie zgodnie z niniejszym Kodeksem Postępowania Certyfikacyjnego lub odpowiednimi przepisami prawa.

Przed zakończeniem swoich usług EID opracowuje plan zakończenia, zawierający następujące postanowienia:

- Zapewni niezbędne środki finansowe, w tym ubezpieczenie odpowiedzialności cywilnej,

do kontynuacji wykonywania czynności odwoławczych.

- Poinformuje o wypowiedzeniu wszystkich podpisujących oraz użytkowników, zaufane strony trzecie i inne AC, z którymi ma umowy lub inny rodzaj relacji, o wypowiedzeniu z co najmniej 6-miesięcznym wyprzedzeniem.
- Odbierze wszelkie upoważnienia podwykonawców do działania w imieniu CA w procedurze wydawania certyfikatu.
- Przeniesie swoje obowiązki związane z utrzymaniem informacji rejestracyjnych i logów w okresie wskazanym użytkownikom.
- Zniszczy lub wyłączy z użytku klucze prywatne urzędu certyfikacji.
- Będzie przechowywać aktywne certyfikaty oraz system weryfikacji i unieważniania do czasu wygaśnięcia wszelkich wydanych certyfikatów.
- Zrealizuje potrzebne zadania w celu przeniesienia obowiązków utrzymania informacji z dziennika i plików dziennika zdarzeń w odpowiednich okresach wskazanych użytkownikowi i podmiotom trzecim, które opierają się na certyfikatach.
- Powiadamiany jest krajowy inspektor z co najmniej dwumiesięcznym wyprzedzeniem o zaprzestaniu działalności i przeznaczeniu certyfikatów, wskazując, czy zarząd zostanie przeniesiony i komu oraz czy też wygaśnie jego ważność.
- Poinformuje również Krajowego Inspektora o wszczęciu postępowania upadłościowego przeciwko EID, a także o wszelkich innych istotnych okolicznościach, które mogą uniemożliwić kontynuację działalności.

6. Kontrola bezpieczeństwa technicznego

EID za pośrednictwem PKI Uanataca S.A. wykorzystuje niezawodne systemy i produkty, zabezpieczone przed wszelkimi zmianami i gwarantujące bezpieczeństwo techniczne i kryptograficzne procesów certyfikacji, dla których są wsparciem.

6.1. Kontrola i instalacja podwójnych kluczy

6.1.1. Tworzenie podwójnych kluczy

Para kluczy pośredniego Urzędu Certyfikacji „EID CA1" jest tworzona przez główny podmiot certyfikujący „UANATACA ROOT 2016" zgodnie z procedurami ceremonii UANATACA, w obrębie przeznaczonego do tego zadania obwodu o wysokim poziomie bezpieczeństwa.

Procedury przeprowadzone podczas ceremonii wygenerowania kluczy zostały zarejestrowane, datowane i podpisane przez wszystkie osoby biorące w niej udział, w obecności Audytora. Te zapisy są przechowywane do celów audytu i obserwacji przez odpowiedni okres.

Urządzenia z certyfikatami FIPS 140-2 poziom 3 i Common Criteria EAL4+ są używane do generowania klucza dla głównego i pośredniego urzędu certyfikacji.

UANATACA ROOT 2016 11	4.096 bitów	25 lat
EID CA1 12	4.096 bitów	13 lat
- Certyfikaty ostatecznego podmiotu	2048 bitów	Do 5 lat

Propagowane dokumenty tekstowe (PKI Disclosure Statement-PDS) wszystkich profili certyfikatów cyfrowych wskazanych w tym dokumencie są dostępne pod linkiem: https://www.electronicid.eu/assets/documents/Texto_de_Divulgacion_para_los_Certificados_de_firma_electr%C3%B3nica_y_autenticaci%C3%B3n_PDS.pdf

6.1.2. Tworzenie podwójnych kluczy dla podpisującego

Klucze podpisującego mogą być generowane przez jego samego za pomocą procedury zdefiniowanej przez EID i które zostaną udostępnione podpisującemu poprzez informacje podane w żądaniu certyfikatu. EID nigdy nie generuje kluczy poza QSCD do wysłania podpisującemu.

Klucze są generowane przy użyciu algorytmu klucza publicznego RSA o minimalnej długości 2048 bitów.

6.1.3. Wysłanie klucza prywatnego do osoby podpisującej

Klucz prywatny osoby podpisującej jest generowany w obszarze prywatnym osoby podpisującej na zdalnym module HSM. Poświadczenia dostępu do klucza prywatnego są wprowadzane przez podpisującego i nie są przechowywane ani nie mogą zostać wydedukowane lub przechwycone przez system

generacji i zdalnej opieki. Klucz prywatny nie jest wysyłany do osoby podpisującej, co oznacza, że nigdy nie opuszcza środowiska bezpieczeństwa, które gwarantuje wyłączną kontrolę nad kluczem prywatnym osoby podpisującej.

6.1.4. Wysłanie klucza publicznego do wystawcy certyfikatu

Metodą przekazania klucza publicznego zaufanemu dostawcy usług elektronicznych jest PKCS#10, inny równoważny dowód kryptograficzny lub inna metoda zatwierdzona przez EID.

6.1.5. Dystrybucja klucza publicznego dostawcy usług certyfikacyjnych

Klucze są przekazywane stronom trzecim, które ufają certyfikatom, zapewniając integralność klucza i uwierzytelniając jego pochodzenie oraz publikując go w Repozytorium.

Użytkownicy mają dostęp do Repozytorium aby uzyskać klucze publiczne, a dodatkowo w aplikacjach S/MIME wiadomość z danymi może zawierać łańcuch certyfikatów, które w ten sposób są rozpowszechniane dla użytkowników.

Certyfikat Głównego i Podrzędnego Urzędu Certyfikacji będzie dostępny dla użytkowników na stronie internetowej EID.

6.1.6. Rozmiar kluczy

- Długość kluczy Głównego Urzędu Certyfikacji wynosi 4096 bitów.
- Długość kluczy Podrzędnego Urzędu Certyfikacji wynosi 4096 bitów.
- Długość kluczy certyfikatów jednostki końcowej wynosi 2048 bitów.

6.1.7. Generowanie parametrów prywatnego klucza

Klucz publiczny głównych, podrzędnych i podpisujących urzędów certyfikacji jest zaszyfrowany zgodnie z RFC 5280.

6.1.8. Sprawdzanie parametrów klucza publicznego

- Długość modułu = 4096 bitów
- Algorytm generowania klucza: rsagen1
- Podsumowanie funkcji kryptograficznych: SHA256.

6.1.9. Generowanie kluczy w aplikacjach informatycznych lub w dobrach kapitałowych

Wszystkie klucze są generowane w dobrach kapitałowych, zgodnie z tym, co wskazano w punkcie 6.1.1.

6.1.10. Cele stosowania kluczy

Klucze do certyfikatów CA służą wyłącznie do podpisywania certyfikatów i list CRL.

Użycie kluczy dla certyfikatów podmiotu końcowego służy wyłącznie do podpisu cyfrowego i nieodrzucenia.

6.2. Ochrona kluczy prywatnych

6.2.1. Standardy modułów kryptograficznych

W odniesieniu do modułów zarządzających kluczami EID oraz użytkownikami certyfikatów podpisu elektronicznego zapewniony jest poziom wymagany przez standardy wskazane w poprzednich rozdziałach.

6.2.2. Kontrola przez więcej niż jedną osobę klucza prywatnego

Do aktywacji klucza prywatnego CA jest wymagana kontrola wieloosobowa. W przypadku niniejszego Kodeksu Postępowania Certyfikacyjnego, wymagane jest ok. 3-6 osób do aktywacji klucza.

Urządzenia kryptograficzne są fizycznie chronione, jak określono w niniejszym dokumencie.

6.2.3. Depozyt klucza prywatnego

EID nie przechowuje kopii użytkowych we własnym zakresie kluczy prywatnych podpisujących.

6.2.4. Kopia zapasowa klucza prywatnego

EID tworzy kopię zapasową kluczy prywatnych urzędów certyfikacji, które umożliwiają ich odzyskanie w przypadku awarii, utraty lub pogorszenia się ich stanu. Wygenerowanie kopii, jak i jej odzyskanie wymagają co najmniej dwóch osób.

Te pliki odzyskiwania są przechowywane w szafach ognioodpornych oraz w zewnętrznym centrum nadzoru.

Wygenerowane klucze: Jedynie jest możliwe tworzenie kopii zapasowych (backups bloob) zaszyfrowanego za pomocą klucza Security World od HSM, a jego odszyfrowanie jest niemożliwe bez użycia poświadczeń, które zna tylko posiadacz certyfikatu.

6.2.5. Archiwizowanie kluczy prywatnych

Klucze prywatne urzędów certyfikacji są archiwizowane przez okres 10 lat od wydania ostatniego certyfikatu. One będą przechowywane w bezpiecznych archiwach ognioodpornych oraz w centrach opieki zewnętrznej. Do odzyskania klucza prywatnego będzie konieczna współpraca przynajmniej dwóch osób z urzędów certyfikacji w początkowym urządzeniu kryptograficznym.

Tylko w przypadku certyfikatów szyfrowanych użytkownik może przechowywać klucz prywatny tak długo, jak uzna to za stosowne. W tym przypadku EID również zachowa kopie klucza prywatnego przypisanego certyfikatowi szyfrowanemu.

EID nie generuje ani nie archiwizuje kluczy certyfikatów wydawanych w oprogramowaniu.

6.2.6. Wprowadzenie klucza prywatnego w module kryptograficznym

Klucze prywatne generowane są bezpośrednio w modułach kryptograficznych.

6.2.7. Sposób aktywacji prywatnego klucza

Klucze prywatne Urzędu Certyfikacji przechowywane są w postaci zaszyfrowanej w modułach kryptograficznych.

6.2.8. Sposób dezaktywacji prywatnego klucza

Klucz prywatny jest aktywowany poprzez wykonanie odpowiedniej procedury bezpiecznego uruchomienia modułu kryptograficznego przez osoby wskazane w punkcie 6.2.2.

Klucze CA są aktywowane przez proces m z n (3 z 6).

Aktywacja kluczy prywatnych Pośredniego urzędu certyfikacji jest zarządzana za pomocą tego samego m procesu, co klucze urzędu certyfikacji.

6.2.9. Sposób niszczenia prywatnego klucza

Aby dezaktywować klucz prywatny, należy wykonać czynności opisane w instrukcji administratora odpowiedniego sprzętu kryptograficznego.

6.2.10. Klasyfikacja modułów kryptograficznych

Przed zniszczeniem kluczy zostanie wydane unieważnienie certyfikatu kluczy publicznych z nimi związanych.

Urządzenia z jakąkolwiek częścią przechowywanych kluczy prywatnych zostaną uruchomione ponownie na niskim poziomie lub fizycznie zniszczone . Aby usunąć zostaną wykonane czynności opisane w instrukcji administratora sprzętu kryptograficznego..

Ostatecznie kopie zapasowe zostaną bezpiecznie zniszczone.

Klucze podpisującego w oprogramowaniu można zniszczyć, usuwając je, postępując zgodnie z instrukcjami aplikacji, która je obsługuje.

Klucze podpisującego znajdują się w sprzęcie i mogą zostać zniszczone za pomocą specjalnej aplikacji komputerowej w siedzibie RA lub EID.

6.3. Inne aspekty zarządzania parą kluczy

6.3.1. Plik klucza publicznego

EID regularnie archiwizuje swoje klucze publiczne, zgodnie z ustaleniami w sekcji 5.5. niniejszego dokumentu.

6.3.2. Okresy używania kluczy publicznych i prywatnych

Okresy użytkowania kluczy to czas określone przez okres ważności certyfikatu, po którym nie mogą być dalej używane.

W drodze wyjątku, jeśli istnieje prywatny klucz deszyfrujący, może być nadal używany nawet po wygaśnięciu certyfikatu.

6.4. Dane aktywacyjne

6.4.1. Tworzenie i instalacja danych aktywacji

Dane aktywacyjne urządzeń zabezpieczających klucze prywatne generowane są zgodnie z postanowieniami pkt. 6.2.2 oraz procedurami ceremonii kluczy.

Tworzenie i dystrybucja takich urządzeń jest rejestrowana.

Ponadto dane aktywacyjne są bezpiecznie generowane.

6.4.2. Ochrona danych aktywacji

Dane aktywacji urządzeń zabezpieczających klucze prywatne głównego i podległego Urzędów Certyfikacji są chronione przez posiadaczy kart administratora modułów kryptograficznych, zgodnie z dokumentem ceremonii klucza.

Osoba podpisująca certyfikat jest odpowiedzialna za ochronę swojego klucza prywatnego za pomocą co najmniej jednego hasła, które powinno być jak najbardziej kompletne i złożone. Osoba podpisująca musi zapamiętać to hasło (hasła).

6.5. Kontrola bezpieczeństwa informatycznego

EID za pośrednictwem infrastruktury klucza publicznego Uanataca, S.A., wykorzystuje niezawodne systemy do świadczenia usług certyfikacyjnych. Wdrożono kontrole i audyty informatyczne w celu ustalenia odpowiedniego zarządzania posiadanymi zasobami komputerowymi z zachowaniem wymaganego poziomu bezpieczeństwa w zarządzaniu elektronicznymi systemami certyfikacji.

W zakresie bezpieczeństwa informacji kontrole są stosowane zgodnie ze schematem certyfikacji systemów zarządzania informacją ISO 27001.

Na wstępie używany sprzęt jest konfigurowany z odpowiednimi profilami bezpieczeństwa przez personel systemu w następujących aspektach:

- Ustawienia zabezpieczeń systemu operacyjnego.
- Ustawienia zabezpieczeń aplikacji.
- Prawidłowe wymiarowanie systemu.
- Konfiguracja użytkowników i uprawnień.
- Konfiguracja rejestru zdarzeń.
- Plan tworzenia kopii zapasowych i odzyskiwania.
- Konfiguracja antywirusów.
- Wymagania dotyczące ruchu sieciowego.

6.5.1. Specyficzne wymagania techniczne dotyczące bezpieczeństwa komputerowego

Każdy serwer zawiera następujące funkcje:

- Kontrola dostępu do usług podległych Urzędów Certyfikacji oraz zarządzanie uprawnieniami.
- Nałożenie rozdzielenia zadań do zarządzania uprawnieniami.
- Identyfikacja i uwierzytelnianie ról związanych z tożsamościami.
- Archiwum historii użytkownika, podległych Urzędów Certyfikacji oraz danych audytowych.
- Audyt zdarzeń związanych z bezpieczeństwem.
- Autodiagnoza bezpieczeństwa związana z usługami podległych Urzędów Certyfikacji.
- Mechanizmy odzyskiwania kluczy oraz system podległych Urzędów Certyfikacji.

Przedstawione funkcjonalności są realizowane poprzez połączenie systemu operacyjnego, oprogramowania PKI, ochrony fizycznej i procedur.

6.5.2. Ocena poziomu bezpieczeństwa informatycznego

Wykorzystywane przez EID aplikacje urzędu rejestracji i certyfikacji są godne zaufania.

6.6. Kontrole techniczne cyklu żywotności

6.6.1. Kontrola rozwoju systemów

Aplikacje są opracowywane i wdrażane zgodnie ze standardami rozwoju i kontroli zmian.

Aplikacje dysponują metodami weryfikacji integralności i autentyczności, a także poprawiania wersji, która ma być używana.

6.6.2. Kontrole zarządzania bezpieczeństwem

EID opracowuje niezbędne działania na rzecz szkolenia i świadomości pracowników w kwestiach bezpieczeństwa. Materiały szkoleniowe i dokumenty opisujące procesy są aktualizowane po zatwierdzeniu przez grupę zarządzania bezpieczeństwem. Do spełnienia tej funkcji posiada roczny plan nauczania.

EID wymaga w drodze umowy środków bezpieczeństwa równorzędnych z każdym zewnętrznym dostawcą zaangażowanym w pracę elektronicznych usług zaufania.

6.6.2.1. Klasyfikacja i zarządzanie informacjami i dobrami materialnymi

Jest prowadzona inwentaryzacja aktywów i dokumentacji, a także procedura postępowania z tym materiałem w celu zagwarantowania jego zużytkowania.

Polityka bezpieczeństwa EID szczegółowo opisuje procedury zarządzania informacjami, w których są one klasyfikowane zgodnie z poziomem poufności.

Dokumenty skatalogowane są na trzech poziomach: NIESKLASYFIKOWANE, DO UŻYTKU WEWNĘTRZNEGO i POUFNE.

6.6.2.2. Operacje zarządzania

EID posiada odpowiednią procedurę zarządzania incydentami i reagowania, poprzez wdrożenie systemu ostrzegania i generowanie okresowych raportów.

Proces zarządzania incydentami został szczegółowo opisany w dokumencie bezpieczeństwa.

EIDS udokumentował całą procedurę związaną z funkcjami i obowiązkami personelu zaangażowanego w kontrolę i manipulację elementami zawartymi w procesie certyfikacji.

6.6.2.3. Traktowanie mediów i bezpieczeństwo

Wszystkie media są traktowane bezpiecznie zgodnie z wymogami klasyfikacji informacyjnej. Podpory zawierające wrażliwe dane są bezpiecznie niszczone, jeśli nie będą ponownie potrzebne.

6.6.2.4. Planowanie systemu

Dział Systemów prowadzi ewidencję możliwości sprzętu. Dzięki aplikacji kontroli zasobów każdego systemu można przewidzieć możliwą zmianę rozmiaru.

6.6.2.5. Raporty o incydentach i odpowiedzi

Istnieje procedura śledzenia incydentów i ich rozwiązywania, w której rejestrowane są odpowiedzi oraz ocena ekonomiczna obejmująca rozwiązanie incydentu.

6.6.2.6. Procedury operacyjne i odpowiedzialności

Zdefiniowane czynności są przypisane do osób pełniących zaufaną rolę, różniących się od osób odpowiedzialnych za wykonywanie codziennych operacji, które nie są poufne.

6.6.2.7. Zarządzanie systemem dostępu

EID dokłada wszelkich możliwych starań, aby poświadczyć, że system dostępu jest ograniczony do osób upoważnionych.

W szczególności:

Ogólny Urząd Certyfikacji (AC)

- Kontrole oparte na firewallach, antywirusach i IDS są dostępne w wysokiej dostępności.
- Wrażliwe dane są chronione za pomocą technik kryptograficznych lub kontroli dostępu z silną identyfikacją.
- W polityce bezpieczeństwa istnieje udokumentowana procedura zarządzania rejestracjami i wypisami użytkowników oraz szczegółowa polityka dostępu.
- Istniejące procedury gwarantują, że operacje są przeprowadzane zgodnie z polityką ról.
- Każdej osobie przypisana jest jedna rola do wykonywania czynności certyfikacyjnych.
- Pracownicy są odpowiedzialni za swoje działania podpisując z firmą umowę o zachowaniu poufności.

Tworzenie certyfikatu

Uwierzytelnienie do procesu wydawania odbywa się za pośrednictwem systemu m do n operatorów do aktywacji klucza prywatnego.

Zarządzanie odwołaniami:

Odwołanie zostanie wykonane poprzez silne uwierzytelnienie do aplikacji autoryzowanego administratora. Systemy logów wygenerują dowody, które gwarantują nieodrzucenie akcji przeprowadzonej przez administratora systemu.

Status odwołania:

W aplikacji stanu odwołania, kontrola dostępu jest oparta na uwierzytelnianiu za pomocą certyfikatów lub podwójnej identyfikacji, aby uniknąć prób modyfikacji informacji o stanie odwołania.

6.6.3. Kontrole bezpieczeństwa cyklu żywotności

EID zapewnia, że hardware kryptograficzny używany do podpisywania certyfikatów nie zostanie manipulowany podczas transportu przez inspekcje dostarczonego materiału.

Sprzęt kryptograficzny jest przemieszczany na przygotowanych stelażach, aby uniknąć jakiejkolwiek manipulacji.

Wszystkie istotne informacje o urządzeniu są rejestrowane w celu dodania ich do katalogu zasobów.

Korzystanie ze sprzętu do podpisywania certyfikatów kryptograficznych wymaga zaangażowania co najmniej dwóch zaufanych pracowników.

Przeprowadzane są okresowe testy testowe w celu zapewnienia prawidłowej pracy urządzenia.

Sprzęt kryptograficzny jest obsługiwany wyłącznie przez zaufany personel.

Klucz prywatny do podpisywania EID przechowywany na sprzęcie kryptograficznym zostanie usunięty po usunięciu urządzenia.

Konfiguracja systemu, jego modyfikacje i aktualizacje są dokumentowane i kontrolowane.

Zmiany lub aktualizacje są dopuszczane przez osobę odpowiedzialną za bezpieczeństwo i znajdują odzwierciedlenie w odpowiednich rejestrach pracy. Te ustawienia zostaną wprowadzone przez co najmniej dwie zaufane osoby.

6.7. Kontrole bezpieczeństwa sieci

Ustanowione są kontrole w celu ochrony fizycznego dostępu do urządzeń zarządzających siecią, a architektura jest wdrożona, która porządkuje generowany ruch w oparciu o jego cechy bezpieczeństwa, tworząc ewidentnie określone sekcje sieci. Podział ten odbywa się za pomocą zapór ogniowych.

Poufne informacje przesyłane przez niezabezpieczone sieci są szyfrowane za pomocą protokołów SSL lub systemu VPN z uwierzytelnianiem dwuskładnikowym.

6.8. Źródła czasu

Procedura skoordynowanej synchronizacji czasu jest dostępna za pośrednictwem NTP, który zapewnia dostęp do dwóch niezależnych usług:

- Pierwsza synchronizacja odbywa się z usługą opartą na antenach i odbiornikach GPS, która zapewnia poziom zaufania STRATUM 1 (z dwoma systemami o wysokiej dostępności).
- Drugi ma synchronizację dodatkową, poprzez NTP, z Królewskim Instytutem i Obserwatorium Wojennym (ROA). **Zmiana statusu bezpiecznego urządzenia do tworzenia podpisów (QSCD).**

W przypadku zmiany statusu certyfikacji urządzeń do składania podpisu kwalifikowanego (QSCD) będzie przebiegać w następujący sposób:

a) Istnieje dostępna lista niektórych certyfikowanych QSCD, a także ścisła współpraca z dostawcami wspomnianych urządzeń w celu zagwarantowania alternatyw w razie możliwej utraty statusu certyfikacji urządzeń QSCD.
b) W przypadku wygaśnięcia okresu ważności lub utraty certyfikatu, niniejsze QSCD nie będą wykorzystywane do wydawania nowych certyfikatów cyfrowych, ani w nowych wydaniach, ani w ewentualnych odnowieniach.
c) Natychmiast nastąpi przejście na urządzenia QSCD z ważną certyfikacją.
d) W przypadku, gdy okaże się, że urządzenie QSCD nigdy nie było, z powodu fałszerstwa lub innego rodzaju oszustwa, niezwłocznie powiadomi swoich klientów i organ regulacyjny, unieważni certyfikaty cyfrowe wydane w tych urządzeniach i zastąpi je, wydając je jako ważne QSCD.

7. Profile certyfikatów i listy unieważnień certyfikatów

7.1. Profil certyfikatu

Wszystkie kwalifikowane certyfikaty wydane w ramach tej polityki są zgodne ze standardem X.509 wersja 3 i RFC 3739 oraz różnymi profilami opisanymi w normie EN 319 412.

Dokumentację związaną z profilami normy EN 319 412 można uzyskać od EID.

7.1.1. Certyfikat ROOT

Urząd roota jest dostępny pod następującym

linkiem:https://web.uanataca.com/common/project/pdf/autoridad-certificacion/01_raiz-ca-2016.cer

```
-----BEGIN CERTIFICATE-----
MIIHAzCCBOugAwIBAgIITWOS6Y7X5ZQwDQYJKoZIhvcNAQELBQAwgbkxCzAJBgNV
BAYTAkVTMUQwQgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3Mg
YXQgd3d3LnVhbmF0YWNhLmNvbS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0Eg
Uy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNBMRswGQYDVQQDDBJVQU5BVEFDQSBS
T09UIDIwMTYxGDAWBgNVBGEMD1ZBVEVTLUE2NjcyMTQ5OTAeFw0xNjAzMTEwOTEz
NTNaFw00MTAzMTEwOTEzNTNaMIG5MQswCQYDVQQGEwJFUzFEMEIGA1UEBww7QmFy
Y2Vsb25hIChzZWUgY3VycmVudCBhZGRyZXNzIGF0IHd3dy51YW5hdGFjYS5jb20v
YWRkcmVzcykxFjAUBgNVBAoMDVVBTkFUQUNBIFMuQS4xFTATBgNVBAsMDFRTUC1V
QU5BVEFDQTEbMBkGA1UEAwwSVUFOQVRBQ0EgUk9PVCAyMDE2MRgwFgYDVQRhDA9W
QVRFUy1BNjY3MjE0OTkwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
```

d5rtQey704cMzz7A1vuB4HLs0Y8YlH7BXKFAuxwzst1GOl7TzZzOeDEjGZMSjI00
JRUdmZ/lmG927tES5dDlrfDrNvKu3mof9j6Wjch4HmNqT6I30TXnhBNbtKEYHWxC
cIvQ0OKaFUUBEt+NzS6smyDAzbwyFUPSPid8JoGaGUMy7hhah38cLN408ffigCFT
ehZIsRvDnsU1WU34vcAYLLmgjsvBNmq2V+Ts8+vtrLcRbpQ8usMbwJSO1aoi71Lu
ISeBGJjqaszMPOty923PGHemImxHl5mHT13k5ha98EK4ZXMFfjxSVrypvpHgjThU
V3s4ZeaSpSbWkFxl6Tl++OTciMLOp66jwZV3I4DqeRmNXJkiRebs5u8bDDZxxeSP
RusoFI1cLm9cqCNy51hd2LNv8QECUNQ/RPon0sh+BSoSedppYXq6TFqpabE/FTnt
JBU7CMJV3EFJ/jSvXf6qj7JjInUQXajSxDdt0WrmDW8aQCRKCZ0Ml/Iwb8yk83/y
ZDt6E+Ez63V/x7sA2ZygG61zf4wOT95FNA4Z1atfOEcp/2uc5HXKrUTXTMDJJZfD
WMo30Ae1Rei94TRd/9XRqPdEk0B/VL5/991SlEX6Ol0NwKRPm6HNNZoWbdnmLEc+
CGnX1yj01R51Y4UTOalJ/W7oiNxmpZQAdAc9NN/gkwIDAQABo4IBCzCCAQcwHQYD
VR0OBBYEFFUs8byhXrnuoC+IVxBb/Jb3kZosMA8GA1UdEwEB/wQFMAMBAf8wgaYG
A1UdIASBnjCBmzCBmAYEVR0gADCBjzAzBggrBgEFBQcCARYnaHR0cDovL3d3dy51
YW5hdGFjYS5jb20vcHVibGljL3BraS9kcGMvMFgGCCsGAQUFBwICMEwMSkNlcnRp
ZmljYWRvIHJhw616IGRlIFVBTkFUQUNBLiBWZXIgaHR0cDovL3d3dy51YW5hdGFj
YS5jb20vcHVibGljL3BraS9kcGMvMA4GA1UdDwEB/wQEAwIBBjAcBgNVHREEFTAT
gRFpbmZvQHVhbmF0YWNhLmNvbTANBgkqhkiG9w0BAQsFAAOCAgEATAyOSKmK/yj6
JFb/RaHMmor8knkwQWVi3lFASKyfLQc6FfHoVjEgihu6HekIlMS7WBzetQVomaTR
TDu6eJeyo/+7CB+VGGHOYYjSdc8F8WI1HFN3f6ztKuM6zlVz3Xyj9BHhg1H4gqNL
Yxe99kq14xQEOR/fm0p7rVgVeeHhG8m1S5UGyyJ1ukeiB0d0PqwVWlG1np+i/nhf
nrxGSTnbRJyHzx6tuaLuQyHQU+Dg0TS8k65a8URioVkQ0CWb7yIyJ5bEBmPR2yqX
Owt6nYR8/3blrU99+wp67pmQttSggX3sB2a9WfY94Y5uIPB7JisOUBmqH23RjakE
c+UMLMjnvJQ82+1M7oGebnaVd1RVK+okemQ5zx57BzkzSl/i4G+Zxya8oQb2cIqF
HnvyCVXDOd4/CWNBLZQCTyGRUKOocvu1kKXgmVY6hTQGhM8Tr5yg/XT21gaAv3/7
th5ib2iGgq8Q8E3AW3ND+8N/qMjZ2aIkBKQYUFmLWiZt6n6ni73E2LQQEs+0uh9+
1xTPcI7AfDv+p0m6HDP0pq0t7BX0DQbh5QwPpiHBkB8atzE5gmQxnkt4/g0S2av5
Lc+U7ufZ5/ao7tLL1qkTX2r87jN7T8+lZOSHBbQan2QosyBfZWXgxaFYTspoy5tP
n4RMcCgXqHSYlArUKaQ8OWmT42AKLdY=
-----END CERTIFICATE-----

7.1.2. Certyfikat CA INTERMEDIA

https://www.electronicid.eu/assets/documents/ELECTRONICIDENTIFICATIONCA1.pem.cer

-----BEGIN CERTIFICATE-----
MIIIZzCCBk+gAwIBAgIIfGPd9OcmVZcwDQYJKoZIhvcNAQELBQAwgZsxCzAJBgNV
BAYTAkVTMQ8wDQYDVQQHDAZNQURSSUQxJzAlBgNVBAoMHkVsZWN0cm9uaWMgSWRl
bnRpZmljYXRpb24gUy5MLjEQMA4GA1UECwwHUFNDLUVJRDEmMCQGA1UEAwwdRUxF
Q1RST05JQyBJREVOVElGSUNBVElPTiBDQTExGDAWBgNVBGEMD1ZBVEVTLUI4NjY4
MTUzMzAeFw0yMDA0MDkxNzM3MDBaFw0yMjA0MDkxNzM3MDBaMIGHMQswCQYDVQQG
EwJFUzEiMCAGA1UEBAwZMWVyLUFwZWxsaWRvIDJkby1BcGVsbGlkbzEPMA0GA1UE
KgwGTm9tYnJlMRgwFgYDVQQFEw9JRENFUy0xMjM0NTY3OFAxKTAnBgNVBAMMIE5v
bWJyZSAxZXItQXBlbGxpZG8gMmRvLUFwZWxsaWRvMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAp89uHcT6Tg00JUsSpNl7YsryG7a40aW/FXtwkFusOlcP
glb7GdmSlYEVO2dYhz1PLHfnvMBOXqp95ftLujZm4uN74vMtPMy6m2VzxLsAH2vW
UJ83q/WQyV8fPCyZJRN+pdnX7cTNx03vmH307OHw6HlxebsXMxrl7j5JTw5wdyry
ZJzG667krsl5Us2kvXq3DNOXng6QdVPodODsRlTJ33WI2h0j9Fuy9B+GgdCXrXt0
nD/FcNkr8LGP+VIzNL1AOe1Jnsa3pJ3jgP9nIWfoisOYC14tP3RCFewHVisurZjw
fWIEvvD0HkDptxWy9Xd4ULpQzPg+tqHZA0SSmpa3ZQIDAQABo4IDvzCCA7swgZsG
CCsGAQUFBwEDBIGOMIGLMAgGBgQAjkYBATALBgYEAI5GAQMCAQ8wCAYGBACORgEE
MFMGBgQAjkYBBTBJMEcWQWh0dHBzOi8vd3d3LmVsZWN0cm9uaWNpZC5ldS9jZXJ0
aWZpY2F0aW9uLXByYWN0aWNlLXN0YXRlbWVudC1jcGQvEwJFTjATBgYEAI5GAQYw
CQYHBACORgEGATCB3gYIKwYBBQUHAQEEgdEwgc4wXAYIKwYBBQUHMAKGUGh0dHBz
Oi8vd3d3LmVsZWN0cm9uaWNpZC5ldS9wdWJsaWMvZG93bmxvYWQvdHNwLWNlcnRp
ZmljYXRlcy9lbGVjdHJvbmljaWRDQTEuY3J0MDYGCCsGAQUFBzABhipodHRwOi8v
b2NzcDEudWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvb2NzcC8wNgYIKwYBBQUHMAGG
Kmh0dHA6Ly9vY3NwMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9vY3NwLzAdBgNV
HQ4EFgQUk+bPyLTDPD3IoBINpHM7ZPRLacowDAYDVR0TAQH/BAIwADAfBgNVHSME
GDAWgBSFFWTNmwdInffmmkQHnHkKjKGWPzAfBgNVHRIEGDAWgRRpbmZvQGVsZWN0

cm9uaWNpZC5ldTCB/wYDVR0gBIH3MIH0MAkGBwQAi+xAAQIwgeYGCysGAQQBg68Z
AQECMIHWMIGEBggrBgEFBQcCAjB4HnYAQwBlAHIAdABpAGYAaQBjAGEAZABvACAA
YwB1AGEAbABpAGYAaQBjAGEAZABvACAAZABlACAAUABlAHIAcwBvAG4AYQAgAEYA
7QBzAGkAYwBhACAAUQBTAEMARAAgAGMAZQBuAHQAcgBhAGwAaQB6AGEAZABvME0G
CCsGAQUFBwIBFkFodHRwczovL3d3dy5lbGVjdHJvbmljaWQuZXUvY2VydGlmaWNh
dGlvbi1wcmFjdGljZS1zdGF0ZW1lbnQtY3BkLzB3BgNVHR8EcDBuMDWgM6Axhi9o
dHRwOi8vY3JsMS51YW5hdGFjYS5jb20vcHVibGljL3BraS9jcmwvZWlkLmNybDA1
oDOgMYYvaHR0cDovL2NybDIudWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvY3JsL2Vp
ZC5jcmwwDgYDVR0PAQH/BAQDAgXgMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEF
BQcDBDAhBgNVHREEGjAYgRZjb3JyZW9AZWxlY3Ryb25pY28uY29tMA0GCSqGSIb3
DQEBCwUAA4ICAQBl1iGUxcndEtFtAY/Z8hwyVtmVJarHWdnfM/eJxCKj4z8Bdl3J
wPh+X9PGXiM7rmBX17GbdBi/YnQLSsNmW6tZWV8SLgEG7qAOeYjIH6Oej8B92zQr
6DwN58ksuDdj4sJ6ZMMDCo3JD85SUNuzbkj+6Fo/hNXyZ5IGj36DKRDZb478W2n4
AMf+/JwLX6wjDO/jOQGGtVHi9kvsKJcStWBgVWFNJkED5CSmik8mDcLtMOYCAqFa
ebe2dgxqBk5vn+JsAKLl2RkSWt7NkcJ9kyYSEfQpg3hUOPLPt3Jq82ppGBaIpz7n
c4UnrHX+DcNO9pgxV6X6fJtjedrahoL4vWSZd5kLUZWIwtfriSFV3A9DvhnJ2OJA
TkSRgr1b01ceuAUvq2d3bWIIWmh//GNIiZViX4kVcbchISVX9PEZBCvs8d7veZ+2
BqjFXvXvayh87430+F71/14pNnaiMllKhkARAKIXvL/cHsW2tVW2idEPNzaYaMvq
5cndubJbfWdcdesgpd3Bj2NSKQpo4Qi09WcuaHwKePq8Ou6kmzNvly1sINMwbspq
/Io73Goe5K01PTT3BCvknexiozhTs1PCuPHmhZJBbk6vDUJsNF8CCOmIBd8NU9/d
Sk9ilQ0ujYrNpdqPDJU7pho59iItV9R+DT0AFL+lOUCgYy3TkynLNGfJJw==
-----END CERTIFICATE-----

7.1.3. Certyfikat Kwalifikowany Osoby Fizycznej w CHMURZE bez QSCD

Pole *Osoby Fizycznej*	CHMURA bez QSCD Uwierzytelnianie i podpis	Obserwacje OID 1.3.6.1.4.1.55193.1.1.1
1. Basic estructure		
1,1. Wersja	"2"	Literał „2" odpowiada wersji 3.
1,2. Serial Number	Automatycznie ustawiane przez CA. Niepowtarzalny numer identyfikacyjny certyfikatu.	Nie może to być liczba ujemna ani 0.
1,3. Signature Algorithm		
1.3.1. Algorithm	SHA-256 with RSA Signature	1.2.840.113549.1.1.11
1.3.2. Parameters	Nie dotyczy	
1,4. Issuer		
1.4.1. Country Name (C)	"ES"	OID 2.5.4.6
1.4.2. Organization Name (O)	"Electronic IDentification S.L."	OID 2.5.4.10
1.4.3. Locality Name (L)	"Madrid"	OID 2.5.4.7
1.4.4. Organization Identifier	"VATES-B86681533"	OID 2.5.4.97
1.4.5. Common Name (CN)	ELECTRONIC IDENTIFICATION CA1.	OID 2.5.4.3
1.4.6. Organizational Unit (OU)	"PSC-EID"	
1,5. Validity		
1.5.1. Not Before	Data rozpoczęcia ważności	YYMMDDHHMMSSZ
1.5.2. Not After	Termin ważności	YYMMDDHHMMSSZ
1,6. Subject		
1.6.1. Country Name	Kraj zamieszkania lub obywatelstwo osoby podpisującej.	OID 2.5.4.6
1.6.2. Organization Name	To pole nie będzie musiało być wypełnione.	OID 2.5.4.10
1.6.3. Organizational Unit Name	To pole nie będzie musiało być wypełnione.	OID 2.5.4.11
1.6.4. Organization Identifier	To pole nie będzie musiało być wypełnione.	OID 2.5.4.97
1.6.5. Title	To pole nie będzie musiało być wypełnione.	OID 2.5.4.12
1.6.6. Surname	Nazwisko osoby podpisującej (jak podano w oficjalnym dokumencie)	OID 2.5.4.4
1.6.7. Given Name	Imię i nazwisko osoby podpisującej (podane w oficjalnym dokumencie)	OID 2.5.4.42
1.6.8. Serial Number	Numer dokumentu urzędowego zakodowany zgodnie z ETSI EN 319 412-1 („IDCES-12345678Z")	OID 2.5.4.5
1.6.9. Common Name	IMIĘ I NAZWISKO OSOBY PODPISUJĄCEJ	OID 2.5.4.3
1,7. Subject Public Key Info		
1.7.1. AlgorithmIdentifier		
1.7.1.1. Algorithm	RSA encryption	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	Nie dotyczy	
1.7.2. SubjectPublicKey	Klucz publiczny osoby podpisującej	

Pole *Osoby Fizycznej*	CHMURA bez QSCD Uwierzytelnianie i podpis	Obserwacje OID 1.3.6.1.4.1.55193.1.1.1
2. Extensions		
2,1. Authority Key Identifier	identyfikator klucza wydawcy	OID 2.5.29.35 (Oznaczony jako NIE krytyczny według z EN 319412-2)
2.1.1. KeyIdentifier		Pochodzące z klucza publicznego
2,2. Subject Key Identifier	Identyfikator klucza osoby podpisującej	OID 2.5.29.14 (Oznaczony jako NIE krytyczny według z EN 319412-2)
2.2.1. KeyIdentifier		Pochodzące z klucza publicznego
2,3. Key Usage		OID 2.5.29.15
2.3.1. Digital Signature	Wybrane „1”	
2.3.2. Content commintment	Wybrane „1”	
2.3.3. Szyfrowanie klucza	Wybrane „1”	
2.3.4. Data Encipherment	Nie wybrane “0”	
2.3.5. Key Agreement	Nie wybrane “0”	
2.3.6. Key Certificate Signature	Nie wybrane “0”	
2.3.7. CRL Signature	Nie wybrane “0”	
2.3.8. Encipher Only	Nie wybrane “0”	
2.3.9. Decipher Only	Nie wybrane “0”	
2,4. Certificate Policies		OID 2.5.29.32 (Oznaczony jako NIE krytyczny według EN 319412-2)
2.4.1. Policy Information		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.55193.1.1.1	Identyfikator polityki EID
2.4.1.2. Policy Qualifiers		
2.4.1.1.1 CPS URI	https://www.electronicid.eu/assets/documents/EID_DPC_v1.r1.pdf	EID CPD URL
2.4.1.1.2. User Notice/Explicit text	„Certyfikat kwalifikacyjny osoby fizycznej w chmurze”.	Tekst wskazujący
2.4.2. Policy Information		
2.4.2.1. Policy Identifier	0.4.0.194112.1.0	Identyfikator polityki certyfikacji kwalifikowanej osoby fizycznej
2,5. Subject Alternative Names		OID 2.5.29.17 (Oznaczony jako NIE krytyczny według z EN 319412-2)
2.5.1. rfc822Name	E-mail osoby fizycznej	
2,6. Extended Key Usage		OID 2.5.29.37 (Oznaczony jako NIE krytyczny według z EN 319412-2)
2.6.1. clientAuth	Obecny (1.3.6.1.5.5.7.3.2)	
2.6.2. Ochrona poczty e-mail	Obecny (1.3.6.1.5.5.7.3.4)	Jest aktywowany tylko wtedy, gdy dołączony jest adres e-mail osoby podpisującej

Pole	CHMURA bez QSCD	Obserwacje OID 1.3.6.1.4.1.55193.1.1.1
Osoby Fizycznej	Uwierzytelnianie i podpis	
2.7. cRLDistributionPoint		OID 2.5.29.31 Ta sekcja nie jest obowiązkowa jeśli funkcjonuje OCSP. (Oznaczony jako NIE krytyczny zgodnie z EN 319412-2
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/eid.crl	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/eid.crl	uniformResourceIdentifier **(NO HTTPS)**
2,8. Authority Info Acces		OID 1.3.6.1.5.5.7.1.1 (Oznaczony jako NIE krytyczny według z EN 319412-2)
2.8.1. Access Description		
2.8.1.1. Acces Method	id-ad-ocsp	OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/	URL dostępu OCSP (NIE HTTPS) uniformResourceIdentifier
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/	URL dostępu OCSP (NIE HTTPS) uniformResourceIdentifier
2.8.2. Access Description		
2.8.2.1. Acces Method	id-ad-calssuers	OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 AccesLocation	https://www.electronicid.eu/assets/documents/ELECTRONICIDENTIFICATIONCA1.pem.cer	Dostęp URL do certyfikatu CA (NIE HTTPS) uniformResourceIdentifier
2,9. Qualified Certificate Statements		OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance		OID 0.4.0.1862.1.1 Wskazanie certyfikatu kwalifikowanego
2.9.2. QcEuRetentionPeriod	"15"	OID 0.4.0.1862.1.3 Okres przechowywania rejestrów
2.9.4. QcPDS		OID 0.4.0.1862.1.5 (SÍ HTTPS) URL dostępu do tekstu informacyjnego
2.9.4.1 PdsLocation		
2.9.4.1.1 url	https://www.electronicid.eu/assets/documents/Texto_de_Divulgacion_para_los_Certificados_de_firma_electr%C3%B3nica_y_autenticaci%C3%B3n_PDS.pdf	
2.9.4.1.2 language	"EN"	URL dostępu do tekstu informacyjnego
2.9.5. QcType	id-etsi-qct-esign	OID 0.4.0.1862.1.6.1 Certyfikat podpisu elektronicznego zgodny z Rozporządzeniem (UE) nr 910/2014
2,10. Basic Constraints		OID 2.5.29.19
2.10.1. cA	FAŁSZYWE	

7.1.4. Kwalifikowany Certyfikat Osoby Fizycznej w CHMURZE z QSCD

Pole *Osoby Fizycznej*	CHMURA z QSCD Uwierzytelnianie i podpis	Obserwacje OID 1.3.6.1.4.1.55193.1.1.2
1. Basic estructure		
1,1. Wersja	"2"	Literał „2" odpowiada wersji 3.
1,2. Serial Number	Automatycznie ustawiane przez CA. Niepowtarzalny numer identyfikacyjny certyfikatu.	Nie może to być liczba ujemna ani 0.
1,3. Signature Algorithm		
1.3.1. Algorithm	SHA-256 with RSA Signature	1.2.840.113549.1.1.11
1.3.2. Parameters	Nie dotyczy	
1,4. Issuer		
1.4.1. Country Name (C)	"ES"	OID 2.5.4.6
1.4.2. Organization Name (O)	"Electronic IDentification S.L."	OID 2.5.4.10
1.4.3. Locality Name (L)	"Madrid"	OID 2.5.4.7
1.4.4. Organization Identifier	"VATES-B86681533"	OID 2.5.4.97
1.4.5. Common Name (CN)	ELECTRONIC IDENTIFICATION CA1.	OID 2.5.4.3
1.4.6. Organizational Unit (OU)	"PSC-EID"	
1,5. Validity		
1.5.1. Not Before	Data rozpoczęcia ważności	YYMMDDHHMMSSZ
1.5.2. Not After	Termin ważności	YYMMDDHHMMSSZ
1,6. Subject		
1.6.1. Country Name	Kraj zamieszkania lub obywatelstwo osoby podpisującej.	OID 2.5.4.6
1.6.2. Organization Name	To pole nie będzie musiało być wypełnione.	OID 2.5.4.10
1.6.3. Organizational Unit Name	To pole nie będzie musiało być wypełnione.	OID 2.5.4.11
1.6.4. Organization Identifier	To pole nie będzie musiało być wypełnione.	OID 2.5.4.97
1.6.5. Title	To pole nie będzie musiało być wypełnione.	OID 2.5.4.12
1.6.6. Surname	Nazwisko osoby podpisującej (jak podano w oficjalnym dokumencie)	OID 2.5.4.4
1.6.7. Given Name	Imię i nazwisko osoby podpisującej (podane w oficjalnym dokumencie)	OID 2.5.4.42
1.6.8. Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCES-12345678Z")	OID 2.5.4.5
1.6.9. Common Name	IMIĘ I NAZWISKO OSOBY PODPISUJĄCEJ	OID 2.5.4.3
1,7. Subject Public Key Info		
1.7.1. AlgorithmIdentifier		
1.7.1.1. Algorithm	RSA encryption	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	Nie dotyczy	
1.7.2. SubjectPublicKey	Klucz publiczny osoby podpisującej	

Pole *Osoby Fizycznej*	CHMURA z QSCD Uwierzytelnianie i podpis	Obserwacje OID 1.3.6.1.4.1.55193.1.1.2
2. Extensions		
2,1. Authority Key Identifier	identyfikator klucza wydawcy	OID 2.5.29.35 (Oznaczony jako NIE krytyczny według z EN 319412-2)
2.1.1. KeyIdentifier		Pochodzące z klucza publicznego
2,2. Subject Key Identifier	Identyfikator klucza osoby podpisującej	OID 2.5.29.14 (Oznaczony jako NIE krytyczny według z EN 319412-2)
2.2.1. KeyIdentifier		Pochodzące z klucza publicznego
2,3. Key Usage		OID 2.5.29.15
2.3.1. Digital Signature	Wybrane „1”	
2.3.2. Content commintment	Wybrane „1”	
2.3.3. Szyfrowanie klucza	Wybrane „1”	
2.3.4. Data Encipherment	Nie wybrane “0”	
2.3.5. Key Agreement	Nie wybrane “0”	
2.3.6. Key Certificate Signature	Nie wybrane “0”	
2.3.7. CRL Signature	Nie wybrane “0”	
2.3.8. Encipher Only	Nie wybrane “0”	
2.3.9. Decipher Only	Nie wybrane “0”	
2,4. Certificate Policies		OID 2.5.29.32 (Oznaczony jako NIE krytyczny według z EN 319412-2)
2.4.1. Policy Information		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.55193.1.1.2	Identyfikator polityki EID
2.4.1.2. Policy Qualifiers		
2.4.1.1.1 CPS URI	https://www.electronicid.eu/assets/documents/EID_DPC_v1.r1.pdf	EID CPD URL
2.4.1.1.2. User Notice/Explicit text	„Certyfikat osoby fizycznej kwalifikowanej chmury z QSCD”	Tekst wskazujący
2.4.2. Policy Information		
2.4.2.1. Policy Identifier	0.4.0.194112.1.2	Identyfikator polityki certyfikacji kwalifikowanej osoby fizycznej
2,5. Subject Alternative Names		OID 2.5.29.17 (Oznaczony jako NIE krytyczny według z EN 319412-2)
2.5.1. rfc822Name	E-mail osoby fizycznej	

Pole *Osoby Fizycznej*	CHMURA z QSCD Uwierzytelnianie i podpis	Obserwacje OID 1.3.6.1.4.1.55193.1.1.2
2,6. Extended Key Usage		OID 2.5.29.37 (Oznaczony jako NIE krytyczny według z EN 319412-2)
2.6.1. clientAuth	Obecny (1.3.6.1.5.5.7.3.2)	
2.6.2. Ochrona poczty e-mail	Obecny (1.3.6.1.5.5.7.3.4)	Jest aktywowany tylko wtedy, gdy dołączony jest adres e-mail osoby podpisującej
2.7. cRLDistributionPoint		OID 2.5.29.31 Ta sekcja nie jest obowiązkowa, o ile istnieje funkcjonalność OCSP. (Oznaczony jako NIE krytyczny zgodnie z EN 319412-2
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/eid.crl	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/eid.crl	uniformResourceIdentifier **(NO HTTPS)**
2,8. Authority Info Acces		OID 1.3.6.1.5.5.7.1.1 (Oznaczony jako NIE krytyczny według z EN 319412-2)
2.8.1. Access Description		
2.8.1.1. Acces Method	id-ad-ocsp	OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/	URL dostępu OCSP (NIE HTTPS) uniformResourceIdentifier
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/	URL dostępu OCSP (NIE HTTPS) uniformResourceIdentifier
2.8.2. Access Description		
2.8.2.1. Acces Method	id-ad-caIssuers	OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Acces Location	https://www.electronicid.eu/assets/documents/ELECTRONICIDENTIFICATIONCA1.pem.cer	Dostęp URL do certyfikatu CA (NOHTTPS) uniformResourceIdentifier
2,9. Qualified Certificate Statements		OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance		OID 0.4.0.1862.1.1 Wskazanie certyfikatu kwalifikowanego
2.9.2. QcEuRetentionPeriod	"15"	OID 0.4.0.1862.1.3 Okres przechowywania rejestrów
2.9.3. QcSSCD		OID 0.4.0.1862.1.4 Urządzenie kwalifikowane do tworzenia podpisów
2.9.4. QcPDS		OID 0.4.0.1862.1.5 (SÍ HTTPS) URL dostępu do tekstu informacyjnego
2.9.4.1 PdsLocation		
2.9.4.1.1 url	https://www.electronicid.eu/assets/documents/Texto_de_Divulgacion_para_los_Certificados_de_firma_electr%C3%B3nica_y_autenticaci%C3%B3n_PDS.pdf	
2.9.4.1.2 language	"EN"	URL dostępu do tekstu informacyjnego
2.9.5. QcType	id-etsi-qct-esign	OID 0.4.0.1862.1.6.1 Certyfikat podpisu elektronicznego zgodny z Rozporządzeniem (UE) nr 910/2014
2,10. Basic Constraints		OID 2.5.29.19
2.10.1. cA	FAŁSZYWE	

7.2. Profil listy unieważnionych certyfikatów

7.2.1. Numer wersji

Listy CRL wydane przez EID są w wersji 2.

7.3. Profil OCSP

7.3.1. Numer wersji

Zgodnie ze standardem IETF RFC 6960.

8. Audyt zgodności

EID poinformowało o rozpoczęciu swojej działalności jako dostawcy usług certyfikacyjnych przez MINISTERSTWO GOSPODARKI I TRANSFORMACJI CYFROWEJ (Sekretariat Stanu CYFRYZACJI I

SZTUCZNEJ INTELIGENCJI - TELEKOMUNIKACJI I INFRASTRUKTURY CYFROWEJ) i podlega przeglądom kontrolnym, które ten organ uzna za konieczne.

8.1. Częstotliwość audytów zgodności

EID przeprowadza audyt zgodności co rok, oprócz audytów wewnętrznych, które przeprowadza według własnego uznania lub w dowolnym czasie, gdy istnieją podejrzenia naruszenia któregokolwiek ze środków bezpieczeństwa.

8.2. Identyfikacja i kwalifikacja audytora

Audyty są przeprowadzane przez niezależną zewnętrzną firmę audytorską, która wykazuje kompetencje techniczne i doświadczenie w zakresie bezpieczeństwa komputerowego, bezpieczeństwa systemów informatycznych oraz audytów zgodności usług certyfikacji kluczy publicznych i związanych z tym elementów.

8.3. Relacja biegłego audytora z badaną jednostką

Wysoko renomowane firmy audytorskie, posiadające działy wyspecjalizowane w przeprowadzaniu audytów komputerowych, więc nie ma konfliktu interesów, który mógłby podważyć ich działania w zakresie EID

8.4. Lista pozycji podlegających audytowi

Audyt sprawdza pod kątem EID:

a) Czy jednostka posiada system zarządzania gwarantujący jakość świadczonej usługi.
b) Czy podmiot przestrzega wymagań Kodeksu Postępowania Certyfikacyjnego oraz innej dokumentacji związanej z wydawaniem certyfikatów.
c) Czy Kodeks Postępowania Certyfikacyjnego i inna powiązana dokumentacja prawna jest zgodna z ustaleniami EID oraz z obowiązującymi przepisami.
d) Czy podmiot odpowiednio zarządza swoimi systemami informatycznymi,

8.5. Działania, które należy podjąć w przypadku braku zgodności

Po otrzymaniu raportu z audytu zgodności przez kierownictwo, wykryte impertynencje są analizowane z firmą, która przeprowadziła audyt, a środki naprawcze są opracowywane i wdrażane w celu usunięcia tych błędów.

Jeżeli EID nie jest w stanie opracować i/lub wykonać działań naprawczych lub jeżeli stwierdzone braki stanowią bezpośrednie zagrożenie dla bezpieczeństwa lub integralności systemu, musi niezwłocznie powiadomić Komisję ds. Bezpieczeństwa EID, która może podjąć następujące działania:

- Tymczasowo wstrzymać operacje.
- Odwołać klucz urzędu certyfikacji i zregenerować infrastrukturę.
- Zakończyć usługę urzędu certyfikacji.
- Inne niezbędne działania uzupełniające.

8.6. Przetwarzanie raportów z audytu

Raporty z wyników audytu przekazywane są do Komisji Bezpieczeństwa EID w ciągu maksymalnie 15 dni od przeprowadzenia audytu.

9. Wymogi prawne

9.1. Zdolność finansowa

9.1.1. Zakres ubezpieczenia

EID posiada gwarancję odpowiedniego zabezpieczenia odpowiedzialności cywilnej, poprzez ubezpieczenie odpowiedzialności cywilnej zawodowej, które utrzymuje zgodnie z obowiązującymi przepisami.

9.1.2. Inne aktywa

Bez zastrzeżeń

9.1.3. Ochrona ubezpieczeniowa użytkowników i osób trzecich, które ufają certyfikatom

EID dysponuje gwarancją wystarczającego ubezpieczenia od odpowiedzialności cywilnej, poprzez ubezpieczenie od odpowiedzialności cywilnej zawodowej, dla zaufanych usług elektronicznych, z ubezpieczeniem minimum 3 000 000 euro.

9.2. Poufność

9.2.1. Poufna informacja

EID będzie uważać za poufne wszystkie informacje, które nie są wyraźnie sklasyfikowane jako publiczne. Informacje uznane za poufne nie są rozpowszechniane bez wyraźnej pisemnej zgody podmiotu lub organizacji, która przyznała im poufny charakter, chyba że istnieje nakaz prawny.

EID utrzymuje należytą politykę postępowania z informacjami oraz wzory umów o zachowaniu poufności, które muszą być podpisane przez wszystkie osoby mające dostęp do informacji poufnych.

9.2.2. Informacje jawne

EID uznaje za informacje jawne:

a) Zawarte w niniejszym Kodeksie Kodeksu oraz Zasadach Certyfikacji
b) Informacje zawarte w certyfikatach.
c) Wszelkie informacje, których dostępność jest zabroniona przez obowiązujące przepisy.

9.2.3. Odpowiedzialność za ochronę informacji poufnych.

EID odpowiada za ochronę poufnych informacji generowanych lub przekazywanych podczas wszystkich operacji. Delegowane strony, takie jak podmioty zarządzające podległymi urzędami certyfikacji lub punktami rejestracji, są odpowiedzialne za ochronę wrażliwych informacji, które zostały wygenerowane lub przechowywane we własnych mediach. W przypadku podmiotów końcowych użytkownicy certyfikatu są odpowiedzialni za ochronę własnego klucza prywatnego oraz wszystkich informacji aktywacyjnych (tj. haseł lub kodów PIN) niezbędnych do uzyskania dostępu lub korzystania z klucza prywatnego.

9.3. Ochrona danych osobowych

EID gwarantuje zgodność z obowiązującymi przepisami o ochronie danych osobowych, odzwierciedlonymi w Rozporządzeniu europejskim nr 2016/679 o ogólnej ochronie danych, Ustawie Organicznej 3/2018 z dnia 5 grudnia o Ochronie Danych Osobowych i gwarancji praw cyfrowych oraz ogólnie, wszelkie obowiązujące przepisy krajowe.

Zgodnie z tym, EID udokumentowała w niniejszym Kodeksie Postępowania Certyfikacyjnego aspekty i procedury bezpieczeństwa i organizacyjne, w celu zagwarantowania, że wszystkie dane osobowe, do których ma dostęp, są chronione przed utratą, zniszczeniem, uszkodzeniem, fałszerstwem oraz bezprawnym lub nieuprawnionym przetwarzaniem.

Następnie wyszczególnione są wszystkie niezbędne informacje dotyczące przetwarzania danych osobowych przez EID:

Organ odpowiedzialny za przetwarzanie danych ELECTRONIC IDENTIFICATION, S.L

CIF: B-86681533
Adres: Avenida Ciudad de Barcelona, 81. 2ª Planta. C.P. 28004 Madrid (Hiszpania).
Email : privacy@electronicid.eu

Cel przetwarzania:

EID ma obowiązek poinformować użytkowników, że wszystkie podane przez nich dane osobowe są przetwarzane w następujących celach:

EID, działając jako kwalifikowany dostawca usług zaufania w zakresie świadczenia elektronicznych usług zaufania i usługi identyfikacji wideo, będzie przetwarzać dane w następujących celach: (i) Prowadzić zarządzanie, rozwój, zgodność i kontrolę stosunku umownego w związku ze świadczeniem Zaufanych Usług Elektronicznych oraz

usługi identyfikacji wideo zgodnie z postanowieniami niniejszego Kodeksu (ii) wysyłanie wszelkiego rodzaju korespondencji pocztowej lub elektronicznej związanej ze wspomnianą relacją; (iii) umieszczenie danych w indeksie kontaktów o charakterze korporacyjnym, wydziałowym i pracowniczym, które tego wymagają; (iv) prawidłowe zarządzanie gospodarcze, księgowe, podatkowe i rozliczeniowe wynikające z utrzymywanego stosunku prawnego; (v) zarządzanie odpowiednimi aktami umownymi w celu archiwizacji i utrzymywania historii akt umownych;
(vi) wydawanie i zarządzanie certyfikatem elektronicznym użytkownika będącego osobą fizyczną; (vii) Elektroniczna identyfikacja użytkowników za pomocą niesamodzielnego wideo, na które, jeśli użytkownik wyrazi wyraźną zgodę, wykorzystamy jego dane biometryczne twarzy na podstawie uzyskania próbki kluczowych punktów danych biometrycznych bez W żadnym momencie EID nie zachowuje wszystkich danych biometrycznych dane. Dane te są pseudonimizowane przy użyciu algorytmu szyfrowania, przy czym tylko dane pseudonimizowane są wykorzystywane do przeprowadzania odpowiednich porównań biometrycznych. W taki sposób informacje związane z tożsamością będą przechowywane, również dane biometrycznego wzoru twarzy w celu umożliwienia przeprowadzenia procesu identyfikacji, który umożliwia EID dostęp do nich i weryfikację tożsamości.

EID informuje, że podane dane osobowe będą przetwarzane wyłącznie w celach opisanych powyżej i nie będą przetwarzane w sposób z nimi niezgodny.

Uprawnienie do przetwarzania

Zasadą traktowania świadczenia Zaufanych Usług Elektronicznych, w tym Usług Identyfikacji Wideo, jest wykonanie umowy żądanych usług, której częścią jest użytkownik.

W przypadku przetwarzania danych biometrycznych, z racji tego, że są to dane szczególnie chronione, opiera się na wyraźnej zgodzie zainteresowanego.

Kategoria danych osobowych

Do kategorii danych osobowych, które przykładowo ale nie wyłącznie mogą być przetwarzane przez EID w celu świadczenia zaufanych usług elektronicznych oraz usługi Identyfikacji wideo należą dane identyfikacyjne (imię, nazwisko i tożsamość), dane kontaktowe (adres pocztowy, e-mail i telefon), dane biometryczne (pozyskiwanie danych biometrycznych i identyfikacyjnych z dokumentu tożsamości użytkownika, ekstrakcja danych biometrycznych z wideo rozmowy oraz porównanie biometryczne między wideo a obrazem dokumentu tożsamości użytkownika.)

Wszystkie podane przez użytkownika dane będą wykorzystywane w celu realizacji usługi weryfikacji tożsamości oraz świadczenia zaufanych usług elektronicznych, a także zarządzania wydawanymi certyfikatami w całym ich cyklu życia.

Okres przechowywania

Dane będą przechowywane przez okres trwania stosunku umownego, o ile nie zażądano ich usunięcia, a także przez okres przedawnienia w przypadku mogących powstać czynności prawnych lub roszczeń, które mogą być dochodzone przez organy urzędowe w związku z umową i po jej zakończeniu. W każdym przypadku maksymalny okres przetwarzania wyniesie 15 lat liczonych od momentu wydania zaświadczenia, chyba że prawo stanowi inaczej. Po zakończeniu relacji dane użytkownika zostaną należycie zablokowane, zgodnie z postanowieniami obowiązujących przepisów.

Odbiorcy

Dane mogą być przekazywane podmiotom trzecim zgodnie z obowiązkami prawnymi, takimi jak: (i) sędziom, sądom oraz siłom i organom bezpieczeństwa, zgodnie z wymogami, zobowiązaniami prawnymi lub w ramach postępowania sądowego; (ii) podmiotom bankowym do zarządzania inkasami i płatnościami; (iii) Agencji Podatkowej, w celu wypełnienia zobowiązań podatkowych; (iv) audytorom finansowym pod kątem przestrzegania zobowiązań finansowych; (v) notariuszom w przypadku upublicznienia dokumentu; oraz (vi) wszelkim innym stronom trzecim, w stosunku do których na mocy obowiązujących w każdym przypadku przepisów konieczne jest wykonanie zlecenia, takich jak właściwe organy administracji, ze względu na kontrolę, rejestrację i inspekcję.

Dane osobowe użytkowników mogą być przekazywane i/lub podane stronom trzecim w wyniku przeglądania list unieważnień lub stronom trzecim, które wymagają konsultacji w sprawie prawidłowości i ważności certyfikatów.

Ponadto niektóre dane mogą być udostępniane podmiotom trzecim, zarówno w Hiszpanii, jak i w Unii Europejskiej, ze względu na usługi, które świadczą naszej firmie (takie jak usługi hostingu danych lub usługi wsparcia identyfikacji), którym zapewnione są odpowiednie środki ochrony, zgodnie z przepisami prawa o Ochronie Danych Osobowych oraz z obowiązkiem zwrotu i/lub zniszczenia do końca świadczenia usługi.

UANATACA przy wydawaniu kwalifikowanych certyfikatów elektronicznych będzie pełnił rolę Kierownika Przetwarzania EID, oferując weryfikację danych zawartych w certyfikacie (nie przetwarza żadnych danych biometrycznych) zgodnie z instrukcjami EID.

Prawa użytkownika

Użytkownikom przysługuje prawo do kontaktu z EID w celu skorzystania z następujących uprawnień w związku z przetwarzaniem ich danych osobowych:

- Potwierdzenie. Wszystkim użytkownikom przysługuje prawo do uzyskania potwierdzenia, czy EID przetwarza dotyczące ich dane osobowe.

- Dostęp i korekta. Użytkownikom przysługuje prawo dostępu do wszystkich danych osobowych, a także żądania sprostowania tych, które są niedokładne lub błędne.

- Usunięcie / anulowanie. Użytkownicy mogą żądać usunięcia/anulowania danych, gdy nie są one niezbędne do celów, dla których zostały zebrane.

- Ograniczenie i sprzeciw. Użytkownik może zażądać ograniczenia przetwarzania, aby jego dane osobowe nie były stosowane w niewłaściwych operacjach. W pewnych okolicznościach i z przyczyn związanych z jego szczególną sytuacją użytkownik może sprzeciwić się przetwarzaniu danych, będąc EID zobowiązany do zaprzestania ich przetwarzania, z wyjątkiem ważnych prawnie uzasadnionych powodów, dochodzenia lub obrony ewentualnych roszczeń.

- Translokacja Zainteresowane strony mogą zażądać, aby ich dane osobowe zostały im przesłane lub przekazane innej odpowiedzialnej osobie, w strukturowym formacie elektronicznym i standardowo używanym.

- Zautomatyzowane decyzje indywidualne: Użytkownik ma prawo nie podlegać decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, a w przypadkach przewidzianych prawem możesz żądać interwencji pracownika.

Aby skorzystać ze swoich praw lub cofnąć zgodę, którą użytkownik wyraził EID, użytkownicy mogą wysłać żądanie na adres e-mail legal@electronicid.eu lub wysłać pismo na adres wskazany w części informacyjnej Administratora. We wspomnianym wniosku należy wyraźnie wskazać prawo, z którego użytkownik pragnie skorzystać. Po otrzymaniu wiadomości, EID skontaktuje się z Użytkownikiem w celu ustalenia jego tożsamości.

Na dodatek, jeśli użytkownik uzna, że jego dane nie zostały przetworzone zgodnie z obowiązującymi przepisami, ma prawo złożyć skargę w Hiszpanii do Hiszpańskiej Agencji Ochrony Danych (www.aepd.es), a także zażądać swoich praw przed wspomnianym organem informacji i ochrony w tym zakresie.

9.3.1. Informacje traktowane jako prywatne

Informacje osobiste o osobie, które nie są publicznie dostępne w treści certyfikatu lub listy CRL, są uważane za prywatne.

9.3.2. Informacje nieuznawane za prywatne

Dane osobowe o osobie dostępne w treści certyfikatu lub listy CRL są uważane za nieprywatne, ponieważ są niezbędne do świadczenia zleconej usługi, bez uszczerbku dla praw przysługujących właścicielowi danych osobowych wynikających z LOPD/RODO.

9.3.3. Odpowiedzialność za ochronę prywatnych informacji

Odpowiedzialność za należytą ochronę prywatnych informacji spoczywa na administratorze danych.

9.3.4. Powiadomienie i zgoda na wykorzystanie informacji prywatnych

Przed rozpoczęciem umownej relacji EID zaoferuje zainteresowanym stronom wstępne informacje o przetwarzaniu ich danych osobowych i prawach oraz w słusznych przypadkach uzyska obowiązkową zgodę na zróżnicowane traktowanie głównego przetwarzania w celu świadczenia umownego usługi.

9.3.5. Ujawnienie na podstawie procesu sądowego lub administracyjnego.

Dane osobowe, które są uważane za prywatne lub nie mogą zostać ujawnione tylko wtedy gdy jest to konieczne do sformułowania dochodzenia lub obrony roszczeń, zarówno w postępowaniu sądowym jak i administracyjnym lub pozasądowym.

Jedynie dane będą mogły zostać ujawnione na podstawie procesu sądowego lub administracyjnego.

9.4. Prawa własności intelektualnej

EID posiada prawa własności intelektualnej do niniejszego Kodeksu, Polityki Certyfikacji i PDS. CPS podległe CA powiązane z hierarchiami EID jest własnością EID, bez uszczerbku dla przeniesienia użytkowania jego praw na rzecz podległych CA i bez uszczerbku dla składek podległych CA, które są ich własnością.

9.5. Ograniczenie odpowiedzialności

EID będzie odpowiadać wyłącznie w przypadku uchybień w procedurach swojej działalności jako Dostawcy Usług Zaufania i zgodnie z postanowieniami odpowiednich Polityk i Praktyk Certyfikacji. W żadnym przypadku nie ponosi odpowiedzialności za działania lub straty poniesione przez wnioskodawców, właścicieli, podmioty korzystające lub, w stosownych przypadkach, zaangażowane strony trzecie, które nie są spowodowane błędami, które można przypisać EID podczas odpowiedniej procedury wydawania i/lub zarządzania certyfikatami.

EID nie ponosi odpowiedzialności w przypadku zdarzenia losowego, siły wyższej, ataku terrorystycznego, dzikiego strajku, a także w przypadku działań stanowiących przestępstwo lub wykroczenie, które mają wpływ na infrastrukturę dostawcy, chyba że wystąpiła poważna wina podmiotu. .

EID nie będzie ponosić odpowiedzialności wobec osób, których zachowanie podczas korzystania z certyfikatów było niedbałe, oraz niezastosowanie się do postanowień Kodeksu Postępowania Certyfikacyjnego, a w szczególności postanowień wyszczególnionych w rozdziałach odnoszących się do obowiązków i odpowiedzialności stron.

Limit pieniężny wartości transakcji wyrażony jest w samym zaświadczeniu podmiotu końcowego. Wyrażenie wartości pieniężnej będzie zgodne z postanowieniami punktu 5.2.2 normy ETSI TS 101 European Telecommunications Standards Institute 862, www.etsi.org

9.6. Klauzury odszkodowawcze

Zgodnie z obowiązującymi przepisami, odpowiedzialność EID i RA nie obejmuje przypadków, w których niewłaściwe użycie certyfikatu ma swoje źródło w zachowaniu przypisywanym użytkownikowi i Stronie korzystającej za:

- Nieudzielenie odpowiednich informacji, początkowo lub później, w wyniku zmian okoliczności odzwierciedlonych w certyfikacie elektronicznym gdy jego niedokładność nie mogła zostać wykryta przez dostawcę usług certyfikacyjnych;
- W wyniku zaniedbania w zakresie ochrony danych tworzenia podpisu i jego poufności;
- Niezłożenie wniosku o zawieszenie lub unieważnienie danych certyfikatu elektronicznego w przypadku wątpliwości co do zachowania poufności;
- Wykorzystaniu podpisu po upływie okresu ważności certyfikatu elektronicznego;
- Przekraczając limity, które widnieją się w certyfikacie elektronicznym.
- W postępowaniu, które można przypisać Stronie Użytkownika, jeśli działa niedbale, gdy nie sprawdza lub nie bierze pod uwagę ograniczeń, które pojawiają się w certyfikacie dotyczących jego możliwych zastosowań i limitów kwotowych transakcji; lub gdy nie bierze pod uwagę statusu ważności certyfikatu.
- Szkody wyrządzone użytkownikowi lub osobom trzecim, którym ufa z powodu niejasności danych zawartych w certyfikacie elektronicznym, jeśli zostały one akredytowane za pomocą dokumentu publicznego, zarejestrowanego w rejestrze publicznym, jeśli jest to wymagane.
- Niewłaściwe lub fałszywe użycie certyfikatu w przypadku, gdy użytkownik/Posiadacz przepisał go lub zezwolił na jego użycie na rzecz osoby trzeciej na mocy czynności prawnej, takiej jak upoważnienie, za które ponosi wyłączną odpowiedzialność użytkownik mający kontrolę nad kluczami powiązanymi z certyfikatem.

EID i RA nie będą również ponosić odpowiedzialności w żadnym przypadku, gdy staną w obliczu którejkolwiek z tych okoliczności:

- Stan wojenny, klęski żywiołowe lub inny przypadek siły wyższej.
- Korzystanie z certyfikatów, o ile wykracza to poza postanowienia aktualnych przepisów i Polityki Certyfikacji
- Z powodu niewłaściwego lub fałszywego użycia certyfikatów lub list CRL wydanych przez CA
- Za korzystanie z informacji zawartych w Certyfikacie lub liście CRL.
- Za szkody wyrządzone w okresie weryfikacji z przyczyn unieważnienia /zawieszenia.
- W przypadku treści podpisanych cyfrowo lub zaszyfrowanych wiadomości lub dokumentów.
- Ze względu na nieodzyskanie dokumentów zaszyfrowanych kluczem publicznym podmiotu.

9.7. Powiadomienia

Wszystkie proponowane zmiany w niniejszej polityce zostaną niezwłocznie opublikowane na stronie internetowej EID.

W tym samym dokumencie znajduje się sekcja dotycząca zmian i wersji, w której można zobaczyć zmiany, które nastąpiły od czasu jego utworzenia oraz datę wspomnianych modyfikacji.

Zmiany w tym dokumencie są przekazywane organizacjom i firmom zewnętrznym, które wystawiają certyfikaty zgodnie z niniejszym Kodeksem. W szczególności zmiany w niniejszym Kodeksie będą zgłaszane organom nadzoru państwowego:

- Hiszpania: Sekretarz Stanu ds. Społeczeństwa Informacyjnego i Indeksu Cyfrowego w Ministerstwie Energii, Turystyki i Indeksu Cyfrowego, czyli takiej, w której w tym czasie mieści się nadzór nad dostawcami usług zaufania.

9.8. Modyfikacje

9.8.1. Mechanizm modyfikacji.

CA zastrzega sobie prawo do modyfikacji tego dokumentu z przyczyn technicznych lub w celu odzwierciedlenia zmian w procedurach, następujących w związku z wymogami prawnymi lub regulacyjnymi (eIDAS, CA/B Forum, Krajowe Organy Nadzorcze itp.) lub w wyniku optymalizacji cyklu pracy. Każda nowa wersja niniejszego Kodeksu zastępuje poprzednie wersje, które jednak nadal mają zastosowanie do certyfikatów wydanych w okresie obowiązywania tych wersji i do pierwszej daty wygaśnięcia tych certyfikatów. Zostanie opublikowana co najmniej jedna roczna aktualizacja. Te aktualizacje zostaną odzwierciedlone w polu wersji u góry dokumentu.

Zmiany, które mogą zostać wprowadzone do niniejszego Kodeksu nie wymagają powiadomienia, z wyjątkiem, gdy będą miały bezpośredni wpływ na prawa podmiotów/użytkowników certyfikatów, w którym to przypadku mogą przesłać swoje uwagi do organizacji zarządzającej polityką w ciągu 15 dni od publikacji.

9.8.2. Okoliczności, w jakich należy zmienić OID.

Nie określono.

9.9. Obowiązujące prawo, skargi i rozwiązywanie konfliktów.

Wszelkie kontrowersje lub konflikty wynikające z tego dokumentu zostaną ostatecznie rozwiązane w drodze arbitrażu przez znawcę, w ramach Hiszpańskiego Sądu Arbitrażowego, zgodnie z jego Regulaminem i Statutem, któremu powierzono administrację arbitrażu i powołanie. znawcy lub trybunału arbitrażowego.

Strony deklarują swoje zobowiązanie do przestrzegania wydanego orzeczenia.

Wykonanie, interpretacja, modyfikacja oraz ważność niniejszego Kodeksu będzie podlegać obowiązującym w każdym monecie przepisom ustawodawstwa hiszpańskiego i Unii Europejskiej.

9.10. Różne klauzury

9.10.1. Całość porozumienia

Posiadacze i strony trzecie, które opierają się na Certyfikatach, w pełni przyjmują treść niniejszego Kodeksu Postępowania Certyfikacyjnego.

9.10.2. Przyznanie

Strony niniejszego Kodeksu nie mogą dokonać cesji swoich praw ani obowiązków wynikających z niniejszego Kodeksu lub obowiązujących umów bez pisemnej zgody EID.

9.10.3. Rozdzielność

Jeśli poszczególne postanowienia niniejszego Kodeksu okażą się nieskuteczne lub niekompletne, nastąpi to bez uszczerbku dla skuteczności wszystkich pozostałych postanowień.

Postanowienie nieskuteczne zostanie zastąpione postanowieniem skutecznym, które uważa się za lepiej oddające sens i cel postanowienia nieprawidłowego. W przypadku niekompletnych postanowień zostanie uzgodniona zmiana, która zostanie uznana za odpowiadającą temu, co zostałoby uzgodnione zgodnie ze znaczeniem i celami niniejszego Kodeksu, gdyby sprawa została wcześniej rozpatrzona.

9.10.4. Zgodność

EID może domagać się odszkodowania i honorariów adwokackich od strony za szkody, straty i wydatki związane z postępowaniem tej strony. Fakt, że EID nie

egzekwuje postanowień niniejszego Kodeksu nie wyklucza prawa EID do późniejszego egzekwowania tych samych postanowień ani prawa do egzekwowania jakiegokolwiek innego postanowienia niniejszego Kodeksu. Aby było skuteczne, każde zrzeczenie musi mieć formę pisemną i być podpisane przez EID.