



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Volkswirtschaftsdepartement EVD
Staatssekretariat für Wirtschaft SECO



SuisselD

Das SuisselD Zertifikat

SuisselD Community Day / Jazoon'10
2. Juni 2010, Zürich




keyon AG
Schlossstrasse 8
8600 Jona
Schweiz
www.keyon.ch


René G. Eberhard
Dept. E-Ing. WTL
Beratungswirtschafts-Ing. FH NDS
CEO, Partner

Tel. +41 55 220 64 03
Mobile +41 79 426 00 45
Fax +41 55 220 64 01
eberhard@keyon.ch

1



SuisselD: Kurz-Steckbrief





Die SuisselD ist:

- ein ZertES-konformes **Signatur-Token**
mit entsprechendem Signatur-Zertifikat,
mit zusätzlich
- einem standardisierten **Authentisierungs-Zertifikat**,
- einer einmaligen **SuisselD-Nummer**
- und einem **SuisselD-Identity-Provider-Service**
- bereitgestellt von einer nach ZertES **zertifizierten
Zertifizierungsdienste-Anbieterin**

EVD/SECO/DSKU/e-Gov KMU

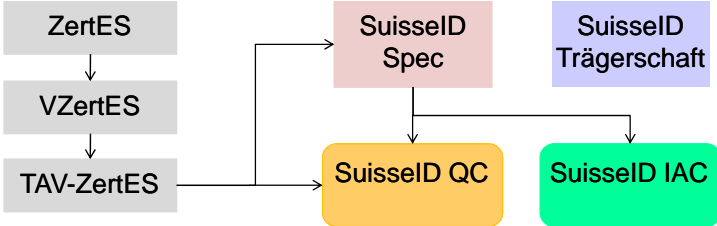
Stabi3IKT::SuisselD

2

 **Grundsatz** 

Basis der SuisselD ist die TAV-ZertES



Sofern die technischen und administrativen Bestimmungen der SuisselD keine ergänzenden oder einschränkenden Angaben machen, gelten die Bestimmungen der TAV-ZertES.



```

graph TD
    ZertES --> VZertES
    VZertES --> TAV_ZertES[TAV-ZertES]
    TAV_ZertES --> SuisselD_Spec[SuisselD Spec]
    TAV_ZertES --> SuisselD_QC[SuisselD QC]
    SuisselD_Spec --> SuisselD_QC
    SuisselD_Spec --> SuisselD_IAC[SuisselD IAC]
    SuisselD_Trägerschaft[SuisselD Trägerschaft] --> SuisselD_IAC
  
```


EVD/SECO/DSKU/e-Gov KMU **Stabi3IKT::SuisselD** 3

 **Grundsatz** 


Die SuisselD Zertifikate sind vertrauenswürdig, weil

- das SuisselD QC gesetzlich geregelt ist
- das SuisselD IAC
 - Die gleiche Benennung der Person hat wie das SuisselD QC
 - Der private Schlüssel sicher, auf dem gleichen Token wie das SuisselD QC, generiert und gespeichert ist

EVD/SECO/DSKU/e-Gov KMU **Stabi3IKT::SuisselD** 4



Definitionen




SuisseID QC

Ein qualifiziertes Zertifikat, das nach den Bestimmungen der ZertES sowie nach den technischen und administrativen Bestimmungen der SuisseID ausgegeben wird.


SuisseID IAC

Ein fortgeschrittenes, nicht qualifiziertes Zertifikat für Identifikation und Authentifizierung, das nach den technischen und administrativen Bestimmungen der SuisseID ausgegeben wird.

EVD/SECO/DSKU/e-Gov KMU
Stabi3IKT::SuisseID
5



Definitionen




Subject DN (Namensgebung)

- Name oder Pseudonym plus
- SuisseID Nummer plus optional
- spezifische Attribute der Inhaberin oder des Inhabers


Der Subject DN eines SuisseID IAC ist immer identisch mit dem Subject DN des korrespondierenden SuisseID QC

SuisseID QC	SuisseID IAC
CN=Hans Muster (Qualified Signature), serialNumber=0001-0000-0000-0001, emailAddress=h.muster@mail.xy	CN=Hans Muster (Authentication), serialNumber=0001-0000-0000-0001, emailAddress=h.muster@mail.xy

EVD/SECO/DSKU/e-Gov KMU
Stabi3IKT::SuisseID
6



Definitionen



SuisseID Nummer 1/2


Eine eindeutige, durch den CSP vergebene Nummer, die einem Zertifikatsinhaber zugeordnet ist.

Beispiel: 0001-9384-9341-8453


Zielsetzung

- Eindeutige Zuordnung eines Zertifikats zu einer Person unabhängig von der Lebensdauer des Zertifikats.
- Für die Applikation transparente Erneuerungsprozesse

EVD/SECO/DSKU/e-Gov KMU
Stabi3IKT::SuisseID
7

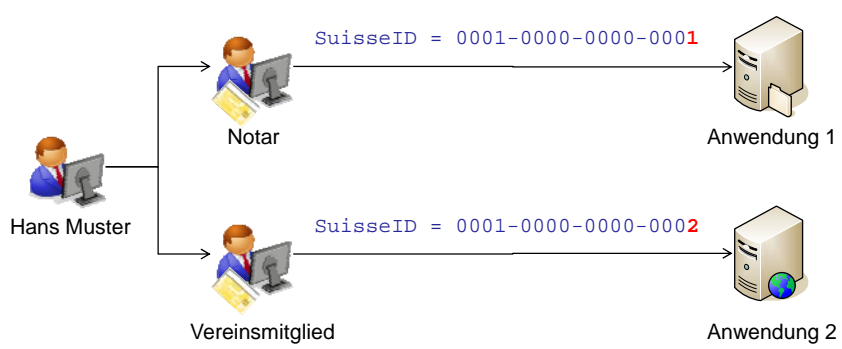


Definitionen



SuisseID Nummer 2/2

Ein Zertifikatsinhaber kann mehrere SuisseID Zertifikate mit unterschiedlichen SuisseID-Nummern beantragen, um diese in unterschiedlichen Kontexten zu nutzen.



```

graph LR
    HM[Hans Muster] --> N[Notar]
    HM --> V[Vereinsmitglied]
    N -- "SuisseID = 0001-0000-0000-0001" --> A1[Anwendung 1]
    V -- "SuisseID = 0001-0000-0000-0002" --> A2[Anwendung 2]
  
```

EVD/SECO/DSKU/e-Gov KMU
Stabi3IKT::SuisseID
8



Definitionen



SuisseID Token

- Das SuisseID QC und das SuisseID IAC befinden sich auf dem **gleichen** Hardware Token.

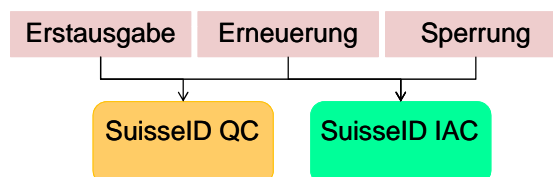



Definitionen / Prozesse




SuisseID Zertifikateset

- Ein SuisseID QC und ein SuisseID IAC, welche jeweils zusammen im Rahmen eines Zertifikatantrags im Bereich der SuisseID ausgegeben werden.
- Alle administrativen Operationen wie z.B. die Erstausgabe, das Sperren und die Erneuerung von SuisseID Zertifikaten, werden immer auf ein SuisseID Zertifikateset angewendet.





Definitionen / Prozesse



SuisseID Zertifikateset

- Die User-Attribute des IDPs beziehen sich auf das SuisseID QC und das SuisseID IAC. Die IDP Attribute sind von der jeweiligen CA qualifiziert signiert.
- 1:1 Beziehung zwischen den IDP Attributen und dem SuisseID QC / IAC

IDP Attribute


SuisseID QC

SuisseID IAC


```

<eCH-0113:attribute
 certIssuerDnQC="C=CH, O=SECO, OU=QC, CN=SuisseId-CSP"
 certSerialNoQC="123456"
 certIssuerDnIAC="C=CH, O=SECO, OU=IAC, CN=SuisseId-CSP"
 certSerialNoIAC="123456"
 name="http://www.ech.ch/xmlns/eCH-0113/1/givennameQc"
 suisseIdNo="1234-1234-1234-1234">
 <icc:givenname>Hans</icc:givenname>
</eCH-0113:attribute>
                
```

EVD/SECO/DSKU/e-Gov KMU
Stabi3IKT::SuisseID
11



Definitionen



CA Hierarchie

Any CA

QC
CA

QC
End entity

SuisseID QC
End entity
SuisseID Policy.1

SuisseID QC
IDP Attribut
SuisseID Policy.3

Any CA

SuisseID
CA

SuisseID IAC
End entity
SuisseID Policy.2

EVD/SECO/DSKU/e-Gov KMU
Stabi3IKT::SuisseID
12



Kennzeichnung der SuisseID Zertifikate

PolicyInformation

Ein SuisseID Zertifikate erkennt man als solches, wenn

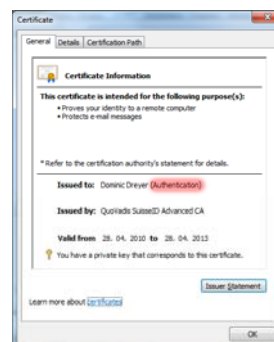
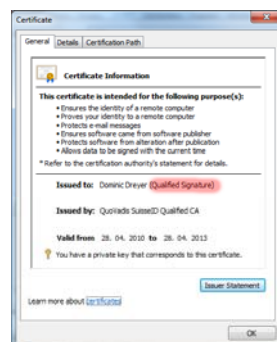
1. dieses durch einen ZertES zertifizierten Anbieter ausgegeben wurde
2. einen SuisseID spezifischen Objektbezeichner (OID) beinhaltet, welche durch das SECO verwaltet wird.



Kennzeichnung der SuisseID Zertifikate

Kennzeichnung

- SuisseID qualified certificate
- SuisseID identity & authentication certificate



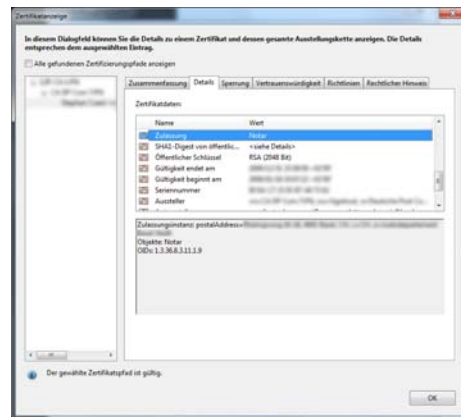


Berufszertifikat für Urkundspersonen



Standardisierter Eintrag: Berufliche Befähigung

- Bezeichnung der Urkundsfunktion (z.B. Notar)
- Bezeichnung der bestätigenden Stelle
- Verweis auf den Eintrag im Register der Urkundspersonen
- Unterstützt von gängigen Applikationen



EVD/SECO/DSKU/e-Gov KMU

Stabi3IKT::SuisseID

15



Windows Logon



Weltweit eindeutiger Microsoft UPN



- UPN := SuisseID-Nr@upn.suisseid.ch
Der Fokus war
- SECO Whitepaper
SuisseID Smart Card Logon
Configuration Guide

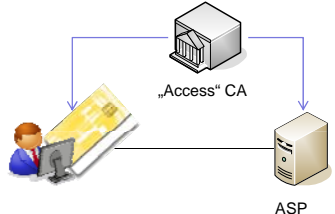


EVD/SECO/DSKU/e-Gov KMU

Stabi3IKT::SuisseID

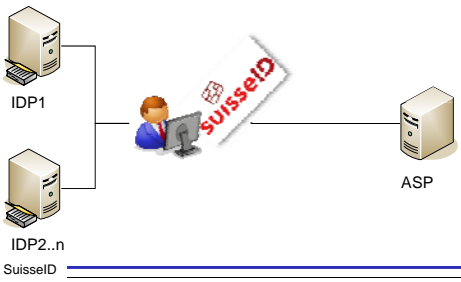
16

 **SuisseID: Unterschiede „Bürgerkarte“** 



- CV Zertifikate
- ICAO Standard
- Spezifische Clientinfrastruktur
- Alle User-Attribute auf Token gespeichert
- Staat „zertifiziert“ ASP für Zugriff auf bestimmte User-Attribute
- User gibt Zugriff auf User-Attribute frei
- Attribute nicht dynamisch erweiterbar



European Citizen Card, Bürgerkarte, ICAO Standard ASP




- X.509 Zertifikate
- „Internet“ Standards (SSL, SAML, etc.)
- Standard Clientinfrastruktur (inkl. Mobile)
- User-Attribute sind im Zertifikat (Auszug) und vollständig im IDP gespeichert
- User gibt Zugriff auf User-Attribute frei
- Attribute und IDP dynamisch erweiterbar

IDP1 IDP2..n SuisseID ASP

EVD/SECO/DSKU/e-Gov KMU **Stabi3IKT::SuisseID** 17



Eine Nummer, eine Person, ein Passwort

Besten Dank für Ihre Aufmerksamkeit

Fragen / Diskussion

EVD/SECO/DSKU/e-Gov KMU **Stabi3IKT::SuisseID** 18