

## A PSD2 szerinti tanúsítvány alapú kommunikáció újdonságai, kihívásai

Paulik Tamás

Public key  
Non repudation certificate  
Qualified e-Signature  
Private key  
Mobile ID  
Trust Service Provider  
Encryption  
QSCD  
Time stamp  
Authentication  
e-Seal  
Certificate Authority

## Az első eIDAS szerint minősített hazai bizalmi szolgáltató

Minősített  
bizalmi  
szolgáltatások

Aláíró tanúsítványok  
Időbélyeg szolgáltatás  
Bélyegző  
Archiválás



Multiplatform  
aláíró  
megoldások

Desktop  
Webes  
Szerver  
Mobil



e-SIGN



Céginformációs  
rendszer

Rendszerfejlesztés

BRIS – európai rendszer

PKI fejlesztés



## Pénzügyi szolgáltatóknak

- PSD2 specifikus tanúsítványok
  - Minősített bélyegző tanúsítvány – dokumentum integritás és hitelesség
  - Minősített webszerver tanúsítvány – biztonságos kommunikációs csatorna
- PSD2 megfelelő SCA eszköz
  - Erős ügyfél-hitelesítés
  - Jóváhagyások





# PSD2

- Payment Services Directive 2
  - 2015/2366/EU
- EU irányelv a pénzügyi szolgáltatások reformjára
- A pénzügyintézeteknek elérhetővé kell tenniük a szolgáltatásaikat harmadik felek számára
- A műszaki kritériumokat külön dokumentum részletezi
  - Regulatory Technical Standards (RTS)

# Regulatory Technical Standards - RTS

- Chapter I. – General provisions
- Chapter II. – Strong Customer Authentication (SCA)
- Chapter III. – Exemptions from SCA
- Chapter IV. – Confidentiality & integrity of the payment service users personalized security credentials
- Chapter V. – Common and secure open standards of communication
- Chapter VI. – Final provisions



## RTS Chapter V. Common & secure open standards of communication

### Articles:

- 28: Requirements for identification
- 29: Traceability
- 30: General obligations for access interfaces
- 31: Access interface options
- 32: Obligations for a dedicated interface
- 33: Contingency measures for a dedicated interface
- **34: Certificates**
- 35: Security of communication sessions
- 36: Data exchanges





## RTS Chapter V. (Comm) – Article 34 Certificates

- Biztosítani kell a hitelességet, integritást és bizalmasságot
- A kommunikációhoz használható
  - eIDAS szerinti minősített bélyegző és/vagy
  - eIDAS szerinti minősített webszerver tanúsítvány (EV)
- Új ETSI szabvány (TS 119 495)
  - Új tanúsítvány profilok
  - Visszafelé kompatibilis módon
  - A Microsec részt vett a kidolgozásában



For the purpose of identification, as referred to in Article 30(1)(a), payment service providers shall rely on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 of the European Parliament and of the Council or for website authentication as referred to in Article 3(39) of that Regulation



# RTS Chapter V. (Comm) – Article 34 Certificates

## Kötelező adattartalom

- Pénzforgalmi hatósági engedélyszám
- Kompetens nemzeti hatóság megnevezése
- Engedélyezett szerepkörök
  - Account servicing payment service provider (ASPSP)
  - Payment initiation payment service provider (PISP)
  - Account information service provider (AISP)
  - Issuing of card based instruments





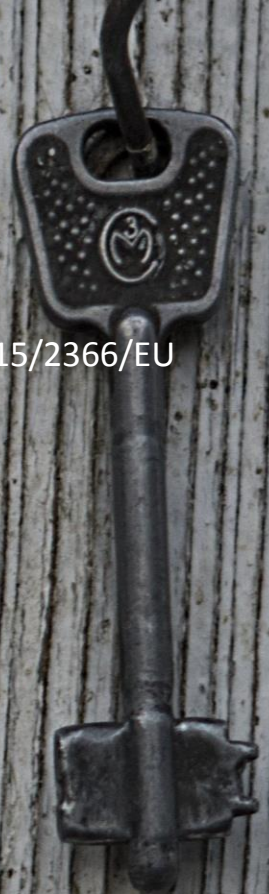
## ETSI TS 119 495

Qualified Certificate Profiles and TSP Policy Requirements under the payment service Directive 2015/2366/EU

A kötelező adattartalom helye a tanúsítványban

Engedélyszám -> organizationidentifier DN mező

Jogosultságok -> új QCStatement





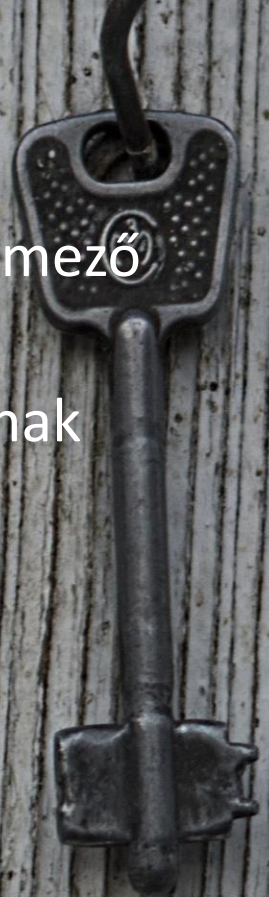
# ETSI TS 119 495 - Engedélyszám

AZ ETSI által előírt ORGANIZATIONIDENTIFIER Subject DN mező további pontosítása

Distinguished Name (DN) – Hierarchikus leírója ez entitásnak

Subject DN – A tanúsítvány alanyának leírója

- SERIALNUMBER = 1.3.6.1.4.1.21528.2.2.99.11647
- E = pelda@penzintezet.hu
- CN = Példa pénzintézet OpenAPI
- **ORGANIZATIONIDENTIFIER = PSDHU-MNB-123456**
- O = Példa Pénzintézet
- L = Budapest
- C = HU





# ETSI TS 119 495 - Szerepkörök

## Új QCStatement

QCStatement: Minősített tanúsítványokban szereplő speciális állítás

### Tartalma:

- Engedélyezett szerepkörök listája
  - Azonosító(OID) + rövid szöveges név
- Hatóság rövid neve (pl.: HU-MNB)
- Hatóság teljes neve angolul





## Biztonságos kommunikáció

- A hálózati kommunikáció „szerver” vége egy minősített webszerver

## De hogyan lesz a kliens autentikáció?

- Aláírt kommunikáció a minősített bélyegzővel
- Tanúsítvány alapú autentikáció
  - „Egyszerű” kliens autentikációs tanúsítvány → nem minősített!
  - Minősített webszerver tanúsítvány kliens üzemmód engedéllyel
    - Nem elterjedt
    - Kettő kell a kulcsmegosztás elkerülése miatt
- Egyéb azonosítás → Account setup



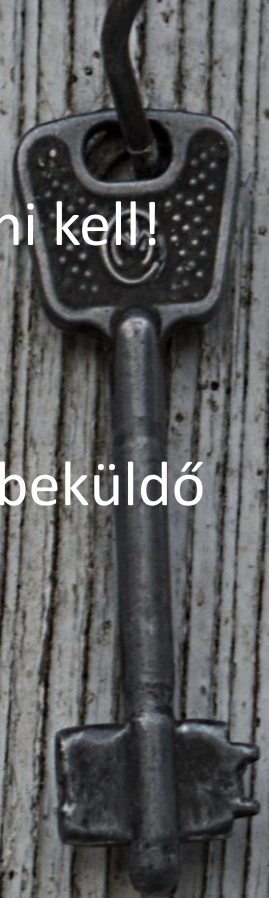


## Jogosultság ellenőrzés

- eIDAS → Minden tanúsítványba kerülő adatot ellenőrizni kell!
- A tanúsítványba kerülő szerepkörök, engedélyszám már ellenőrzöttek!
- Befogadáskor a tanúsítvány alapján eldönthető, hogy a beküldő rendelkezik-e a szükséges szerepkörrel

## Passporting

- Szerepkörök kérése idegen országban
- Eltérhet az otthoni szerepköröktől!
- **A tanúsítványban viszont csak az otthoni szerepkörök vannak benne!**





## Aláírt üzenetek

- A hiteles csatornán átjövő kérés eredete később körülményesen bizonyítható
- Aláírt kérések esetében a kérés archiválható, így utólag fel lehet mutatni
- PSD2 elvárás a nyílt, szabványos megoldások használata

Milyen aláírás formátumok használhatóak?

Milyen aláírható formátumok használhatóak?

Mire kell figyelni archiváláskor?





## Aláírás formátumok

- Az ETSI több szabványos elektronikus aláírás formátumot definiál
  - Bináris formátum
    - CMS Advanced Electronic Signature (CAAdES)
  - XML formátum
    - XML Advanced Electronic Signature (XAdES)
  - PDF formátum
    - PDF Advanced Electronic Signature (PAdES)
- Nem ETSI szabványos, de elterjedt formátumok
  - XMLDSIG (W3C)
  - JSON Web Signature





# Aláírható formátumok

- Különálló aláírás: Az aláírás az állomány mellett külön állományban foglal helyet
- ASiC → ZIP benne állományok és különálló aláírások
- PDF → PAdES aláírással
- SOAP-XML → XMLDSIG aláírással
- JSON Web Token → JSON Web Signature





## Archiválás

- Elektronikusan aláírt dokumentumok archiválása
  - Aláírt dokumentum
  - Tanúsítvány
  - Visszavonási információk
  - Időpont (minősített időbélyeg)
- Az aláírt dokumentum, benne a tanúsítvánnyal kliens oldalon készül
- Az visszavonási információk és az időbélyeg rákerülhet
  - Kliens oldalon: Nő a csomagméret és sok erőforrást igényel
  - Szerver oldalon: Kötegelhetően végezhető





## PSD2 specifikus teszt tanúsítványok

- Európában csak két CA tud jelenleg a PSD2 teszt tanúsítványokat biztosítani
  - Minősített bélyegző
  - Minősített webszerver
  - Minősített webszerver kliens üzemmóddal
  - Kliens autentikációs tanúsítvány
- Tetszőleges PSD2 adattartalommal  
Ország, Felügyelet, Engedélyszám, Szerepkörök
- PKI tanácsadás

<https://www.microsec.hu/szolgalattasok/psd2.html>





A long-exposure photograph of a city street at night. The image shows multiple lanes of traffic with light trails from cars and motorcycles. Tall buildings with lit windows line the street, and streetlights illuminate the scene. A semi-transparent dark blue banner is overlaid across the middle of the image.

**Paulik Tamás**  
**paulik@microsec.h**

Köszönöm a figyelmet!