ANSSI

Standardisation supporting sectorial certification – The eIDAS stories

21 january 2019

Certification of QSCDs under eIDAS – Where are we ?

>What we have

- **Recognized protection profiles** for « **user managed** » QSCDs (e.g. smart cards)
- **Mutual recognition** of certified QSCDs

>What we need

- **Recognized standards** (*and a slight review of the regulation*) for « **remote signing** » QSCDs
- Rules for **managing the security during the lifecycle** of QSCDs

Managing the security over the lifecycle of QSCDs

>**Limit the duration** of a QSCD's conformity certificate

>Enforce **periodic vulnerability assessment**

>Take into account that **the QSCD may need to be updated** (e.g. by having in scope of evaluation the patch mechanisms & processes)

>**Require commitment from the developer** to

- monitoring CVEs & published vulnerabilities,
- performing impact analysis on changes,
- communicating with CBs, SBs, CERTs and customers,
- etc...

Going further than QSCDs

>**Other areas of the eIDAS regulation** where mandatory certification would help :

- **trustworthy systems and products** used by QTSPs (notably cryptographic devices)
- **electronic identification means** (especially for level of assurance high)

>*Considerations on managing the security over the lifecycle of QSCDs apply there as well*

Contacts

Agence nationale de la sécurité des systèmes d'information
Romain Santini
romain.santini@ssi.gouv.fr
supervision-eIDAS@ssi.gouv.fr
Suivez notre actualité : Twitter - LinkedIn

Version 1.0 – 21/01/2019