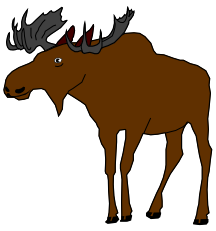


Standards support

- 🛡️ **Rec. ITU-T X.50x | ISO/IEC 9594-13, *Decentralized public-key infrastructure***
 - 🛡️ **Rec. ITU-T X.510 | ISO/IEC 9594-11, *Protocol specifications for secure operations***
 - 🛡️ **Rec. ITU-T X.1080.0, *Access control for telebiometrics data protection***
 - 🛡️ **Plus, what communication protocol support is needed for the health credential support**
-

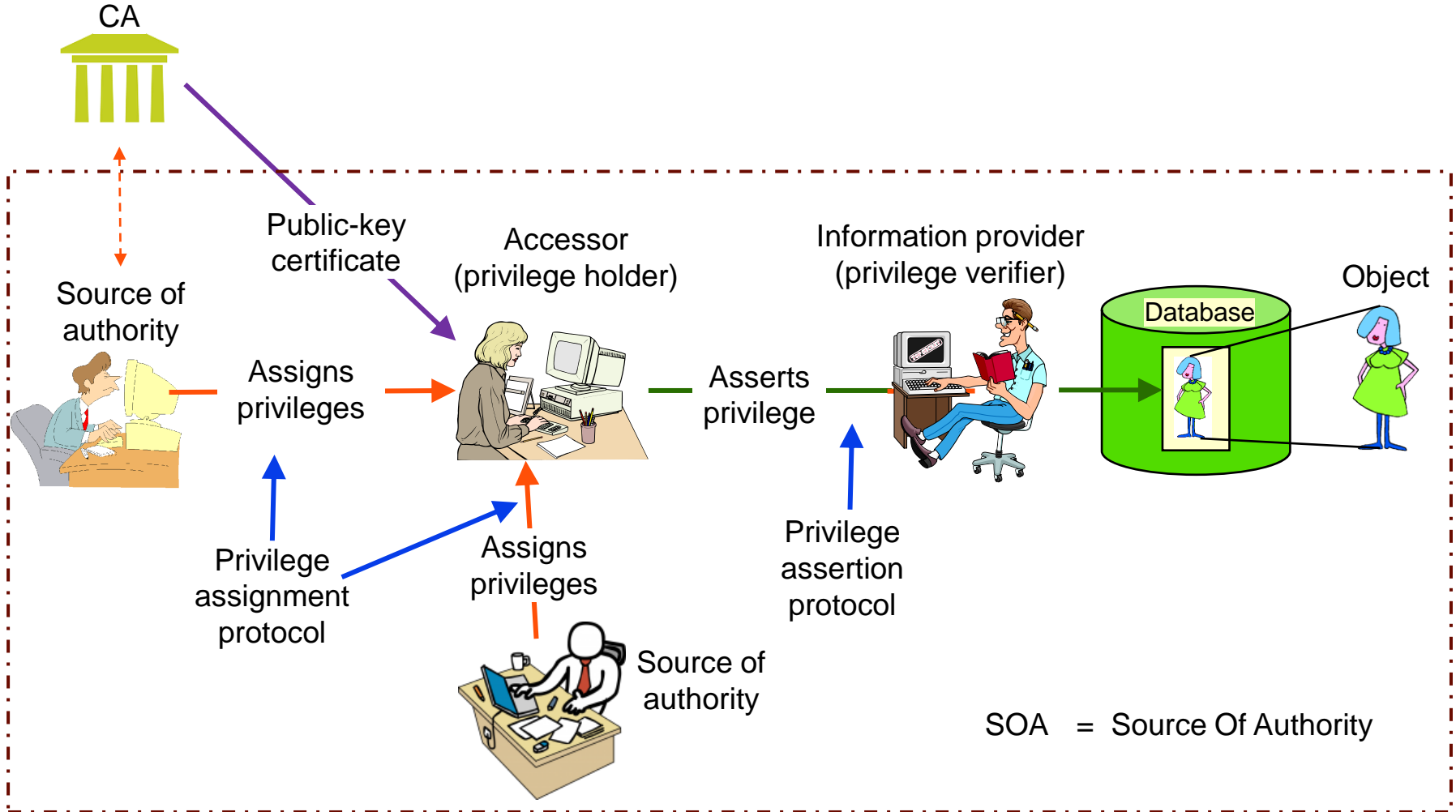


Access control

- 👍 **Based on a Need-to-Know**
 - 👍 **A service-oriented view**
 - 👍 **Type of object accessed (e.g., journal)**
 - 👍 **Access of specific objects (e.g., what journal(s))**
 - 👍 **Type of operation allowed (e.g., read, update)**
 - 👍 **Privileges are assigned in attribute certificate signed by proper authority**
 - 👍 **Identity assured by public-key certificate**
-

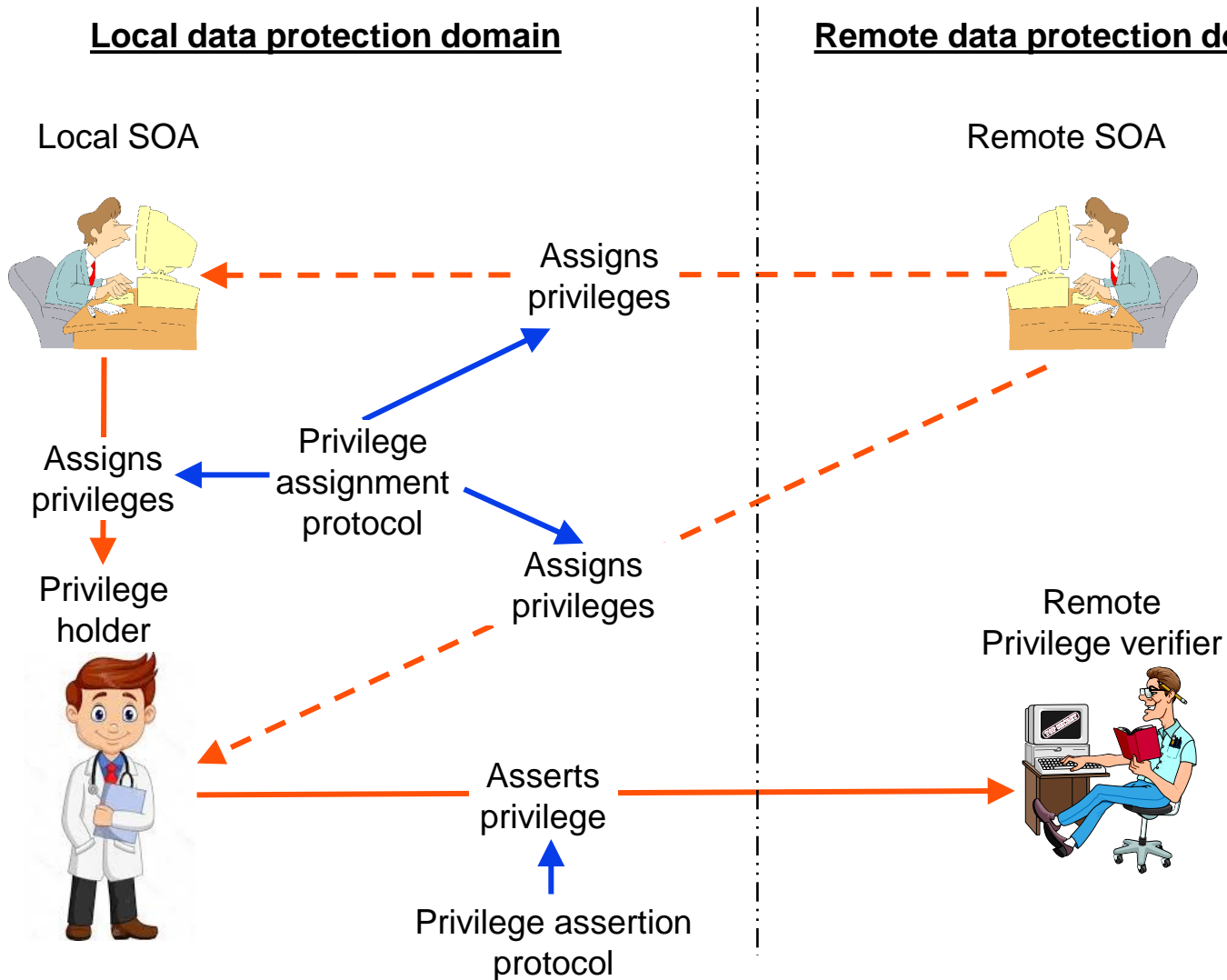


Single privacy protection domain model





Cross domain privileges



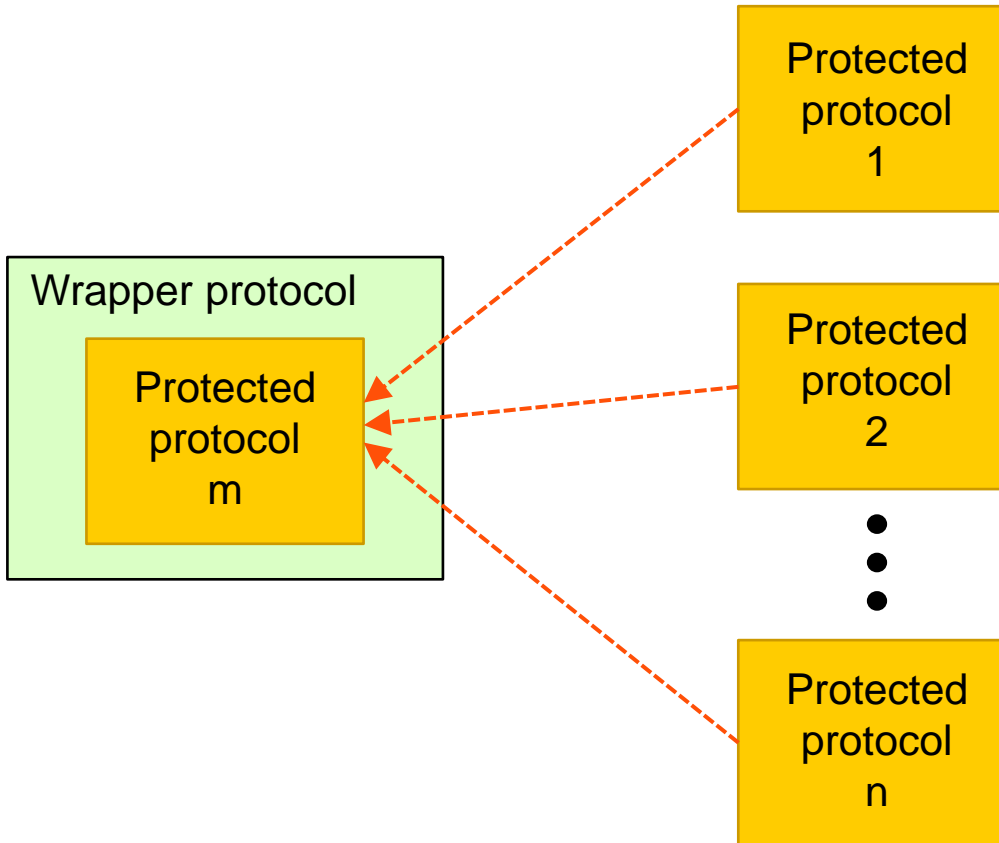


Rec. ITU-I X.510 | ISO/IEC 9594-11

Wrapper protocol

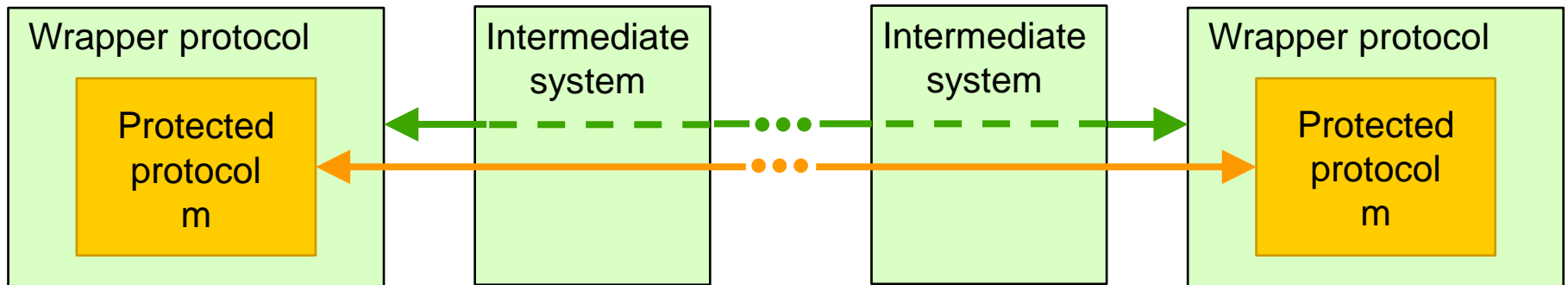


Protected protocol plug-in



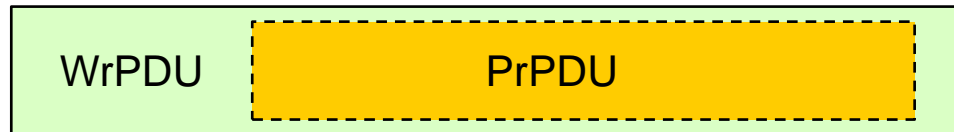


Communications structure





APDU structure





Wrapper handshake

Digital signature algorithm

-----|

Public-key certificate(s)

-----|

Symmetric keys establishment

-----|

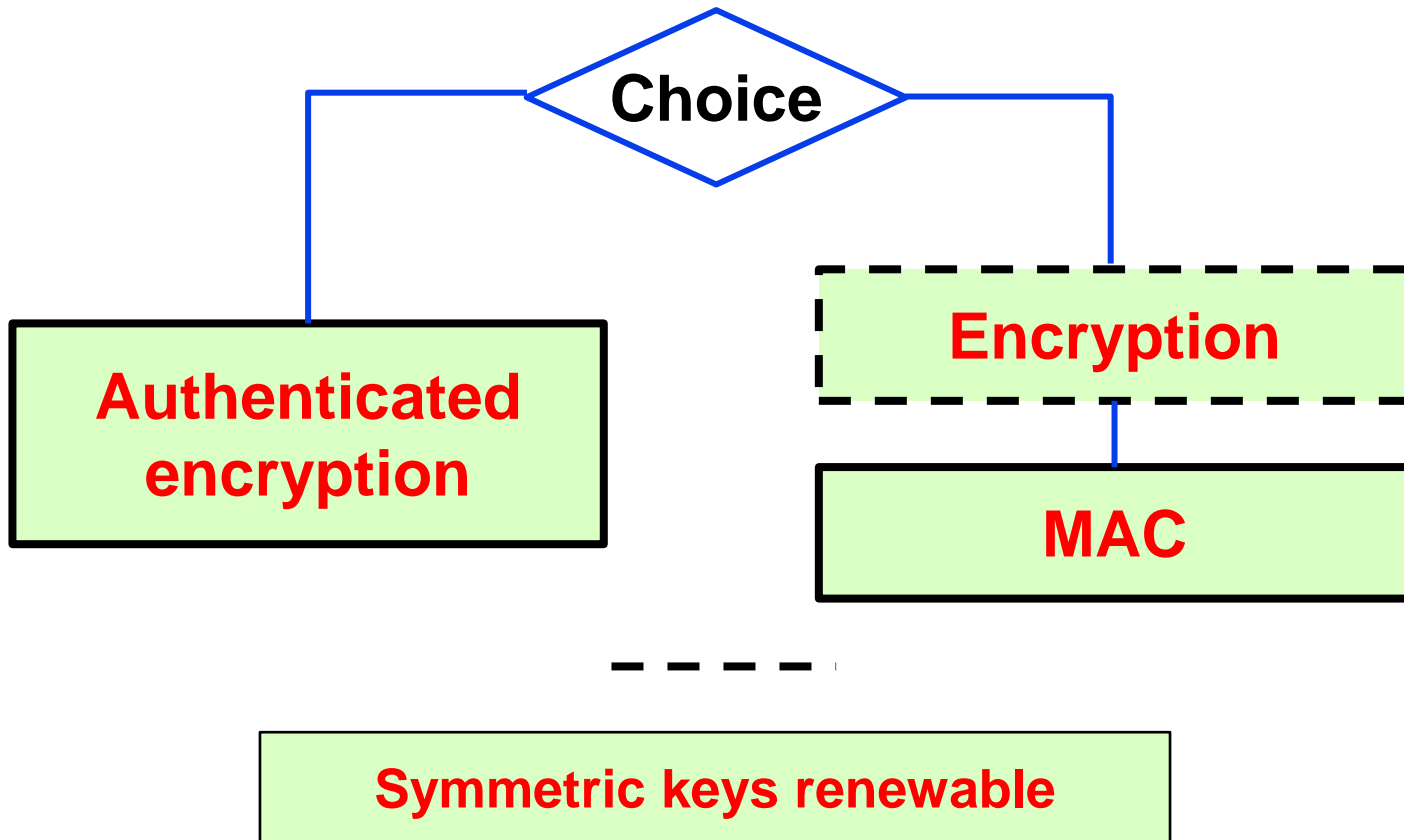
Type of data protected

-----|

Digital signature



Protect during data phase












The devil is in the details

A large, faded illustration of a red devil with horns, a tail, and a pitchfork, standing next to a black cauldron. The devil is smiling and looking towards the viewer. The illustration is centered in the background of the slide.

**Migration strategies for
cryptographic algorithms**
**(Migration to quantum-safe
algorithms)**



The quantum computer threat to cybersecurity

-  **The threat is primary against asymmetric algorithms**
 -  **Digital signature algorithms**
 -  **Key establishment algorithms**
 -  **Private key can be disclosed if sufficient computer power is available**
 -  **The threat is less for symmetric algorithms**
 -  **Doubling the key size seems sufficient**
 -  **Can be a problem for constrained devices**
-



The strategy (Cont.)



The alternative algorithm and associated information shall be specified in such a way that a back level recipient can ignore it



A back level recipient will ignore the alternative algorithm, but validate according to the native one



An advanced recipient will verify according to the alternative algorithm



At the end of the migration period, the alternative algorithm becomes the new native algorithm



Request/response paradigm

