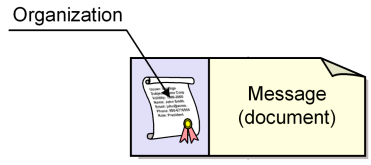
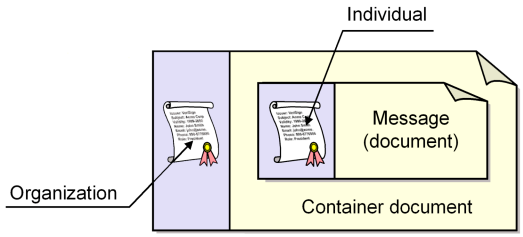
# Signing B2B-Messages

According to current "PKI-theology", employee-certificates and keys should be used for signing B2B-messages. However, this scheme is not aligned with current pre-PKI inter-organization transaction-systems like the ones used by banks all over the world as well as by manufacturer-supplier networks, that almost exclusively authenticate messages on *business-partner level* rather than on employee level. The following figures show an alternative, on-line adapted PKI-architecture that can evolve from a very basic level, to supporting PKI of arbitrary complexity. In addition, the described schemes allow TTPs to efficiently support a PKI market, as the foundation is built on certificates for stable entities like individuals and organizations, while dynamic data like "employment" is automatically handled by *internal* information systems rather than by being engraved in static certificates. *The organization-signatures, are in all variants to be performed by internal business systems* (servers) rather than by individuals, to be compatible with current business systems, as well as not making "an individual = organization".



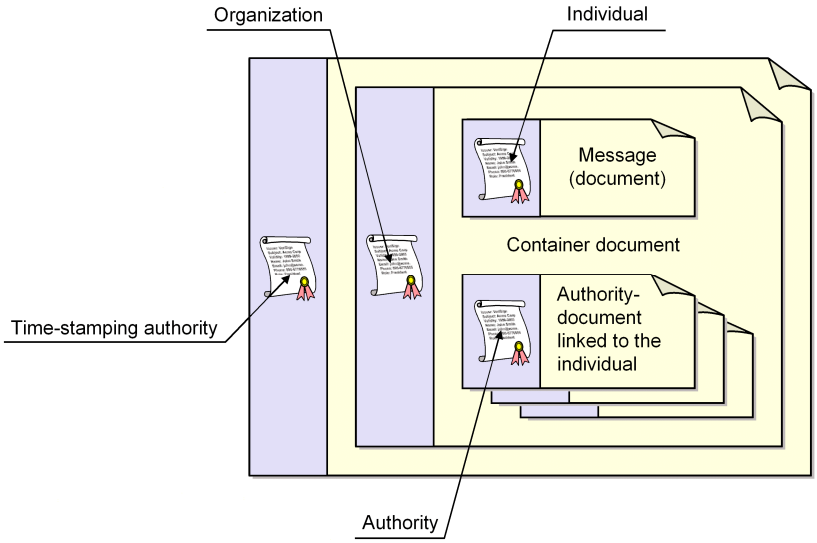

**Basic**

The following scheme (together with SSL/TLS-communication) is a PKI-equivalent to the leased lines, shared secrets, and VPNs used for securing 99.9% of current e-transactions. This scheme is particularly suited to the B2B-field as *it is comparatively simple*, *supports employee privacy*, is *independent of particular client-security solutions*, *supports automated business processes*, as well as being fully *compatible with the emerging "Web Services" technologies*




**Advanced**

Dual-signed messages work like "virtual" employee-certificates as the outer organization-signature vouch for the association to the enclosed individual's signature. The container-document may contain additional attributes like authorization data for the individual. This scheme is compatible with all current signature laws




**"Full Dossier"**

Elaborate scheme where external authorities vouch for the individual's role (like M.D.). This scheme is suited for advanced inter-organization workflow where each step inserts the previous step in order to create a complete image of each process step. XML Schemas are very suitable for this "Russian Doll" type of messaging

Notation: The following symbols are used in the diagrams:

A message or document. Typically XML-formatted, based on XML Schema(s)

A digital signature and associated X509.v3 certificate(s). Typically using XML DSig formatting

V1.02, December 2002

Author's e-mail address: anders.rundgren@telia.com, Phone: +46 70 - 627 74 37