SSL facilities in FlexiNet

Laurence Jordan

Getting Security

Q. I want secure communication in a client-server system - what shall I use?

A. SSL:

- An industry standard protocol.
- Off-the-shelf implementations.
- They plug straight into your application.

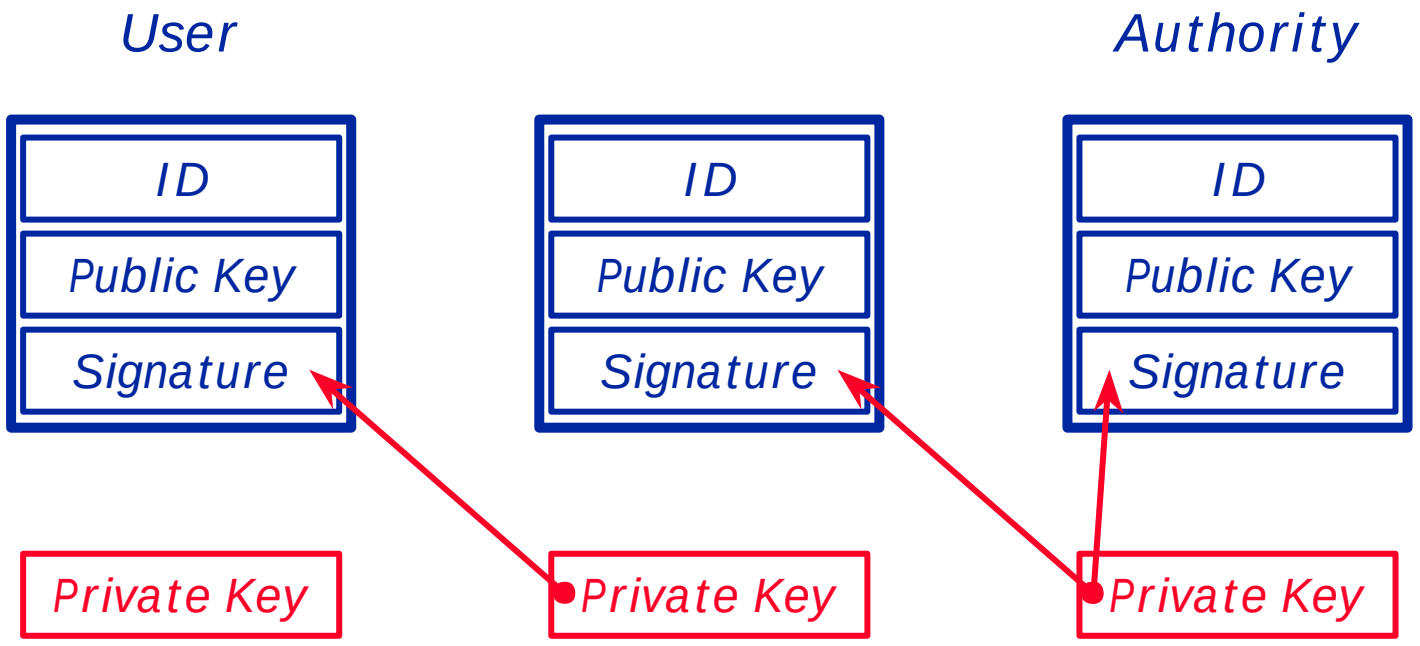
Authentication

Q. What assurance is there of identity?

A. The client gets a certificate chain from the server which the client can verify.

The server can also demand a certificate chain from the client and verify that.

A certificate chain



Confidentiality

Q. Is the communication secure from eavesdropping?

A. SSL encrypts data using a negotiated algorithm.

Unfortunately, if you have an SSL implementation which is subject to export restrictions, the encryption strength is really rather poor.

Integrity and Nonrepudiation

Q. Does SSL detect message tampering?

A. SSL uses message authentication codes to detect changes to the message in transit.

Q. If the owner of the client or server later denies that a message was sent, can that be detected?

A. That's outside the scope of SSL.

Access Control

Q. If I want to control access to server interfaces, refusing connections from unauthorized clients, can SSL help?

A. You could use different sockets for the different interfaces, with different configurations.

Using SSL

Q. How easy is it to integrate SSL into an existing system?

A. Simply replace the sockets used in the existing system with SSL sockets, and add the appropriate configuration data.

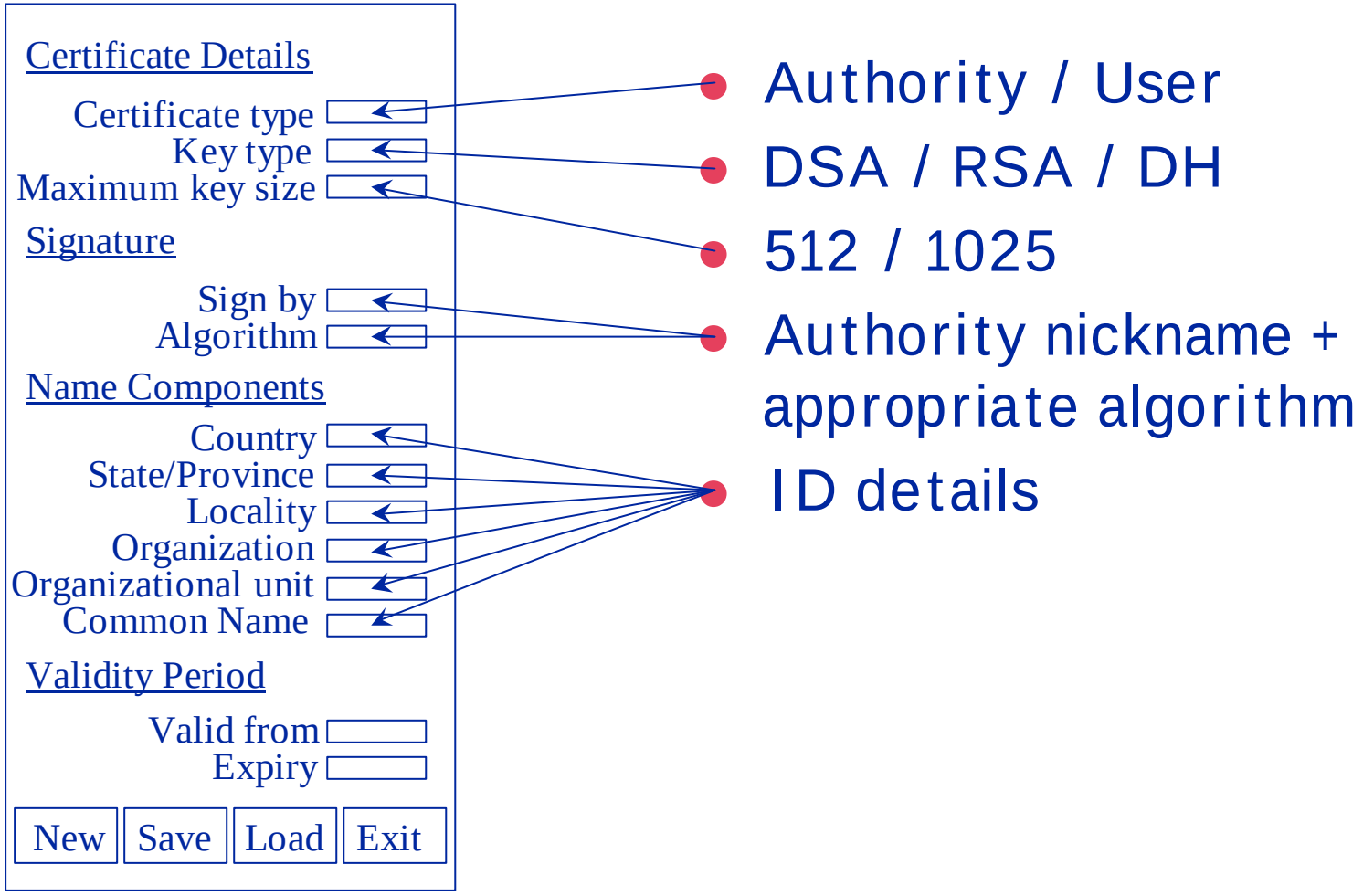
SSL has to be set up for the algorithms you are willing to use, and the authentications required.

Certificate Management

Q. Does SSL help with handling and maintaining certificates?

A. No.

The Certificate GUI



Conclusions

- New (SSL) sockets for old:
  - It does not cover all possible security needs

    (TLS may improve on this).
  - If the security required cannot be captured in a server SSL configuration - you have problems to solve.

And...

- Certificates!
  - Certificate management problems -

    it's more than just issuing certificates.
  - Revocation is still a difficult problem, and an applications should be written to cope with the revocation procedure.

Finally

It is generally easier to design the system around your security requirements than to try to retro-fit security afterwards.