

SafeStick®

ZoneBuilder White Paper

General Summary

ZoneBuilder provides single sign on to SafeStick on trusted computers within the company network. Users can change lost passwords and set up trust relationships with team workers.

Security is based on PKI and users certificates.

Compatible with PKI with smart cards or E-tokens.

Revision

Johan Söderström

Original document creation

2008-04-17

ZoneBuilder Features

Single Sign On

To increase the ease of use, ZoneBuilder technology provides automatic logon to SafeStick from Windows user accounts. The transparency to the user is then 100%. Using SafeStick will not differ from the use of any standard USB flash disk. The security is still intact though and all information will remain protected.

Trusted Team Members

A user in a project working environment is able to create trusts with other team members. This will allow automatic logon also for the users trusted team members. In this way, no user will have to give out their private password to their team members. The function will also make file sharing more effective between all members in a team.

Security Overview

Security

Zonebuilder works on a PKI basis. To create single sign on to SafeStick on an account it has to be trusted. SafeStick is configured to trust a specific root CA. Any account with a certificate and a private key from that CA is considered trusted. When a trust relationship is set up, SafeStick will authenticate the computer with the private key and unlock.

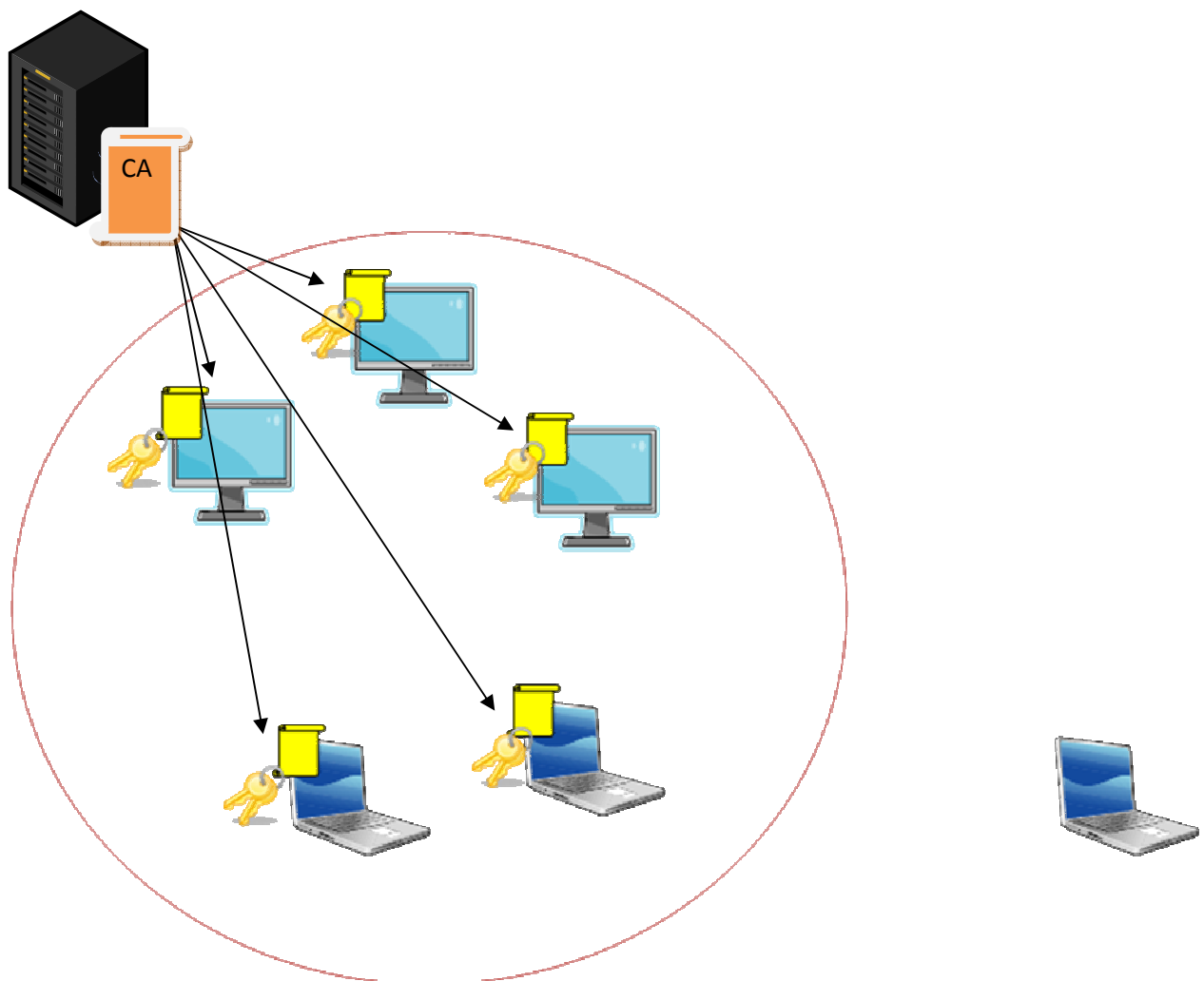
Infrastructure

Each account associated with ZoneBuilder needs a unique certificate installed. This will ensure that single sign on cannot be established on computers not trusted by the company.

Building the Zone

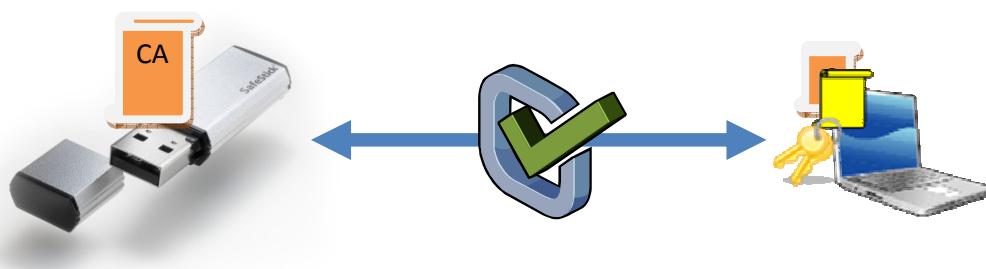
Certificates are deployed with the Auto Enrollment feature from a Windows Server equipped with a CA and Certificate Services. Enrollment can also be accomplished with an Automatic Certificate Request GPO in Windows Server 2000 or 2003.

The enrollment is made to either computers or users in Active Directory.

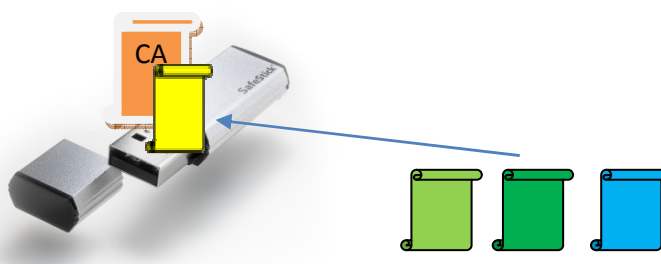


Setting Up Trusts

SafeStick is equipped with the public CA certificate from the initial configuration. When SafeStick is set up on first time use with a user, it will verify the host computer with the preloaded certificate by checking for a valid certificate chain.



Once the computer/account is verified it will be considered the host computer for this user and SafeStick will load this certificate into its trusted list.



The trust procedure can be repeated on all computers/accounts with a valid certificate signed by the trusted CA, thus enabling the user to set up zones with team workers. When the user leaves a team the trusted certificates can easily be removed from the trusted list on SafeStick.

Any certificate that has been revoked or passed its valid date will be rejected since the certificate chain in this case is not valid.

Contact

BlockMaster AB
Jutahusgatan 8
222 29 Lund
046-276 51 00
info@blockmaster.se

Johan Söderström
CTO
046-276 51 05
0735-00 00 75
johan@blockmaster.se