



NetIQ Advanced Authentication Framework

Security and Encryption Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
Architecture	4
Components	5
Authentication Flow	5
Disconnected mode	6
Data Storage and Encryption	7
Data Storage	7
Session Management	7
Storage of biometric data	8
Communication Channels	8
Auditing and Logging	9
Index	10

Introduction


About This Document


Purpose of the Document


This Security & Encryption Guide is intended for administrators and security officers and describes the security and encryption protocols used in NetIQ Advanced Authentication Framework.


For more general information on NetIQ Advanced Authentication Framework™ and the authentication software you are about to use, see NetIQ Advanced Authentication Framework – Client User's Guide.

Document Conventions

 **Warning.** This sign indicates requirements or restrictions that should be observed to prevent undesirable effects.

 **Important notes.** This sign indicates important information you need to know to use the product successfully.

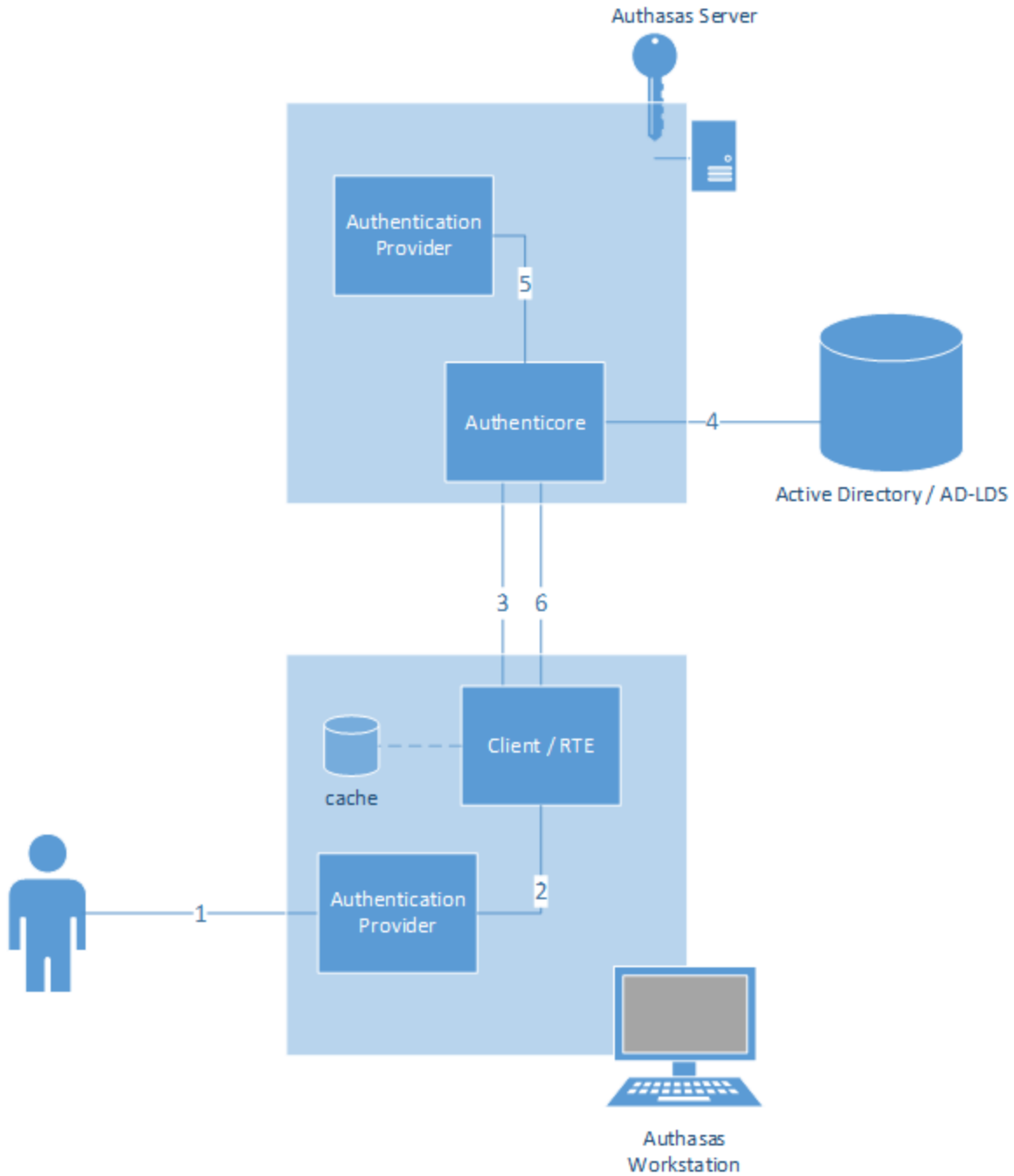
 **Notes.** This sign indicates supplementary information you may need in some cases.

 **Tips.** This sign indicates recommendations.

- Terms are italicized, e.g.: ***Authenticator***.
- Names of GUI elements such as dialogs, menu items, buttons are put in bold type, e.g.: the **Logon** window.

Architecture

This chapter describes the high-level architecture of NetIQ Advanced Authentication Framework and the components that participate in the authentication process. It also describes the authentication flow.



Components

NetIQ workstation is a client computer with NetIQ components installed and used for strong authentication.

Authentication Provider is a component responsible for capturing authentication credentials, computing a hash or creating a template on the clientside and verifying or identifying the credential on the server side.

NetIQ Client is a component that must be installed on every NetIQ-secured workstation. It allows users to enroll authenticators and to authenticate in their operating systems using enrolled authenticators.

NetIQ RTE (Run Time Environment) allows to use the SDK (Software Developer Kit) with no need to install NetIQ Advanced Authentication Framework Client component. It is useful when you would like to use NetIQ Advanced Authentication Framework to secure access to certain applications only, without changing the regular Windows logon procedure.

NetIQ Authenticore Server is responsible for user data processing, particularly for the user authentication process. It also stored audit information in the Windows eventlog.

Active Directory is used to store the user credentials and NetIQ user settings.

AD-LDS (Active Directory-Lightweight Directory Services) is a separate application partition used to store user credentials and NetIQ user settings. This is used when it is not possible to extend the Active Directory itself.

Authentication Flow

1. The user presents their credentials, this can be a username and fingerprint, contactless card, password, OTP token or any other supported authentication method.
2. The Authentication Provider receives the credential and depending on the authentication method used performs some actions. This can be creating a fingerprint template out of a fingerprint to hashing the credential for further use.
3. The Client then sends the credential including the time, source and authentication provider identifier to the Authenticore server.
4. The Authenticore server searches the user and retrieves the enrolled credential from the repository.
5. The Authentication Provider matches the user credential with the enrolled credential and checks with Active Directory if the user is authorized.

6. If all is verified and ok the Authenticore server returns the domain username and password to the client which is then used to authenticate to Windows or any other authentication event.

Disconnected mode

NetIQ supports the caching of credentials. After a successful authentication to NetIQ the credentials are cached on the local hard drive. More information about caching of credentials can be found in the *Administrative Tools - Administrator's Guide*.

1. The user presents his/her credentials, this can be a username and fingerprint, contactless card, password, OTP token or any other supported authentication method.
2. The Authentication Provider receives the credentials and depending on the authentication method used performs some actions. This can be creating a fingerprint template out of a fingerprint to hashing the credential for further use.
3. The Client detects that it is not connected to the domain or an Authenticore server and tries to authenticate the user to the local cache. The Authentication Provider matches user's credentials with the cached credentials. If all is verified and ok, Client does a cached logon using the domain username and password.

Data Storage and Encryption

In this chapter:

- [Data Storage](#)
- [Session management](#)
- [Storage of biometric data](#)
- [Communication channels](#)

Data Storage

While installing the first NetIQ server, the configuration wizard asks for the level of encryption. NetIQ can use any of the installed Microsoft Cryptographic Service Providers (CSP). The following configurations are supported by default but if an organization wants to use their own encryption level this is possible.

Algorithm	Base CSP	Strong CSP	Enhanced CSP
Hash function			
MD2	128 bits	128 bits	128 bits
MD4	128 bits	128 bits	128 bits
MD5	128 bits	128 bits	128 bits
SHA1	160 bits	160 bits	160 bits
SHAMD 5 SSL3	288 bits	288 bits	288 bits
Data encryption			
DES	56 bits	56 bits	56 bits
RC2	40 bits	40 bits	128 bits
RC4	40 bits	40 bits	128 bits
3DES TWO KEYS	Not supported	112 bits	112 bits
3DES	Not supported	168 bits	168 bits
Data signing			
RSA	512 bits	512 bits	1024 bits

Session Management

Only after successful authentication a user can get access to its encrypted credentials. Per user a separate encryption key is used so it is impossible for other users or administrators to access the encrypted user credentials of another user than themselves.

Storage of biometric data

NetIQ Advanced Authentication Framework never stores the actual fingerprint in its secure encrypted storage. A calculation is made from the minutia points and used in a one way algorithm to create a template. This template is stored in encrypted form in the secure storage. It is impossible to create a fingerprint image from the template.

Communication Channels

NetIQ Advanced Authentication Framework secures communication channels in order to assure confidentiality and the integrity of the transmitted data.

The three communication channels are each secured by different mechanisms.

1. Client RTE <-> Authentication Provider <-> Authenticore Server

Communications in this channel use Microsoft Remote Procedure Calls (RPCs), and the ncalrpc protocol sequence with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY flag set to ensure the confidentiality and integrity of the transmitted data.

Additional information about RPC can be found in the Microsoft article "Remote Procedure Call" located at: <http://msdn2.microsoft.com/en-us/library/ms950395.aspx>

2. Client / RTE <- -> Authenticore Server

Communications in this channel use Microsoft Remote Procedure Calls (RPCs), and the ncacn_ip_tcp protocol sequence with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY flag set to ensure the confidentiality and integrity of the transmitted data.

Additional information about RPC can be found in the Microsoft article "Remote Procedure Call" located at: <http://msdn2.microsoft.com/en-us/library/ms950395.aspx>

3. Authenticore Server <- -> Active Directory / AD-LS

This communication channel uses the Microsoft Active Directory Service Interfaces (ADSI).

Information about ADSI is available in the Microsoft article "Active Directory Service Interfaces" at:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adsi/adsi/active_directory_service_interfaces_adsi.asp

Auditing and Logging

NetIQ Advanced Authentication Framework provides extensive event trapping and reporting using the Windows Event Log as the repository for information about:

- Application errors
- Successful and unsuccessful authentication attempts
- Object access
- System intrusion

Events for NetIQ Advanced Authentication Framework are logged on the machine on which they occur and are also stored in the central logservers.

When a client is disconnected, all events will be cached and when connection is re-instated to the LogServer, all events will be synchronised. This provides a full audit trail even for disconnected devices.

Index

A

Active Directory 5, 8
Administrator 6
Application 9
Authentication 1, 3-6, 8-9
Authenticator 3
Authenticore server 5

C

Client 3, 5-6, 8

D

Data 7

L

Logon 3

O

OTP 5-6

R

Remote 8
RTE 5, 8

S

Security 1, 3
Server 5, 8
Software 5
System 9

W

Windows 5-6, 9