nevisAuth: Secure Authentication

nevisAuth implements strong user and system authentication for identity and access management solutions. It offers secure execution of multi-step authentication and is able to dynamically adjust authentication strengths. nevisAuth is highly flexible and integrable and supports plug-ins to various authentication methods.

Functions & Tasks

- Central authentication service
  - Central user and system authentication for nevisProxy or any third-party access gateway
  - Identity provider for the federation of identities in distributed environments
- Multi-step authentication
  - Workflow configuration via integrated state engine
  - State transfers (internal or via login mask)
  - State engine with configurable transfer and branching
- Offers user authentication with any type of credential, independent of an application’s capabilities
- Supports variable authentication strengths including dynamic set-up
  - Fine-grained timeout handling compliant with authentication strength
- Issues signed tokens for propagation (end-to-end security)
- Creation/procedure of SAML 1.1/2.0 identity assertions
- Ensures end-to-end security through identity propagation

Product Highlights

Flexible and easily expandable
- Modular architecture: authentication core and plug-ins
- Various standard plug-ins to connect to peripherals included in standard product delivery
- Customer-specific plug-ins can be integrated/developed

Auditability (auditing framework)
- Compliance-relevant actions are recorded: login, logout, re-authentication, failures, etc.
- Auditing framework supports integration of customer-specific plug-ins for the processing of audit events

Easily configurable
- Configuration via easy-view XML file
- Integrated into nevisAdmin

Configuration of workflows
- Can be set up to manage several access channels
- Self-administration and registration services
- Configurable login dialogs with arbitrary input or selectable text elements for every authentication step
- Optional integration of error reports, values of previous entries, or output of plug-ins to login dialogs

Supported authentication methods
- User name/password
- User certificates
- Scratch list/rastercard
- Biometric tokens
- OTP tokens
- Challenge/response
- Mobile devices
Technical Highlights

Integration features
- Pluggable authentication backends
- Pluggable backends for the management of users, roles and resources: Oracle, LDAP, Xindice
- Active Directory integration
- Supports Windows-Kerberos
- Integrates RADIUS-based services
- Supports SecurID, Vasco, SafeWord tokens
- Supports rastercards in combination with nevisIDM
- Optional use of hardware security modules (HSM) for all crypto operations
  - HSM integration via PKCS#11
- Integration with nevisAdmin management console

Technical data
- Based on Java
  - Standalone
  - Java EE container deployment
- Webservice, Radius and WS-Trust interface
- Delivery as nevisAppliance (software appliance) or software for Solaris/Linux

Strong References

E-banking
nevisAuth is deployed by renowned financial institutions such as UBS and PostFinance to secure their e-banking solutions.

SSO portals
nevisAuth authenticates the users of major Swiss e-business and e-government SSO portals such as the single sign-on portal of the FDJP (Federal Department of Justice and Police) or PostLogistics’ business customer portal “My Post Business”.

AdNovum Informatik AG
Stephan Schweizer, Nevis Product Manager
Roentgenstrasse 22, 8005 Zurich
Phone +41 44 272 61 11
info@adnovum.ch, http://www.adnovum.ch