How to Secure Remote Access to Internal Resources

Presentation of mobile signature based solution
ETRONIKA RADIUS Adapter (ERA)

ETRONIKA

Problem

Static passwords may be **the weakest** link in your network security exposing your sensitive data and applications to online fraudsters. The growing need for a much **stronger** virtual proof of **identity** is **evident** across all industries wherever confidential data and resources are involved.

Conclusion:
When number of remote users increases and the use of VPN connection accelerates, static passwords must be replaced by much more secure user identification means.

Mobile Signature Replaces Static Passwords?

- **Mobile signature** is a component of **two-channel authentication solution** that requires two elements to establish user's identity: user's credentials and mobile phone with mobile signature.

- Based on proven wPKI (Wireless Public Key Infrastructure) technology, mobile signature protects user login and ensures access for authenticated users only.

- The use of mobile signature is an alternative to one-time password generators.

Solution

ETRONIKA RADIUS Adapter (ERA) solution enables the usage of mobile signature to identify and authenticate remote user.

The ERA solution is designed keeping in mind that users need comfortable and simple self-identification means, and IT administrators anticipate reliable, secure and easy to maintain application.

Where to Use

ETRONIKA RADIUS Adapter (ERA) could be used for:

- Remote access via VPN connection to company's intranet or extranet
- Access to network devices that use RADIUS protocol for authentication

Why It's Better

Quick and easy implementation procedure

ETRONIKA RADIUS Adapter will interface with any RADIUS client and web application **without additional programming**. This solution resides on your server and involves **minimal setup** and management.

What is RADIUS?

Networking protocol that provides centralized authentication, authorization of the network clients and accounting of the network processes management. The RADIUS server authenticates users or devices before granting them access to a network, authorizes those users or devices for certain network services, and makes account for usage of those services.

Optimal maintenance costs

No additional devices, password generators or media for mobile signature are required.

ERA is **compatible** with many firewalls, access servers and RADIUS based VPN.
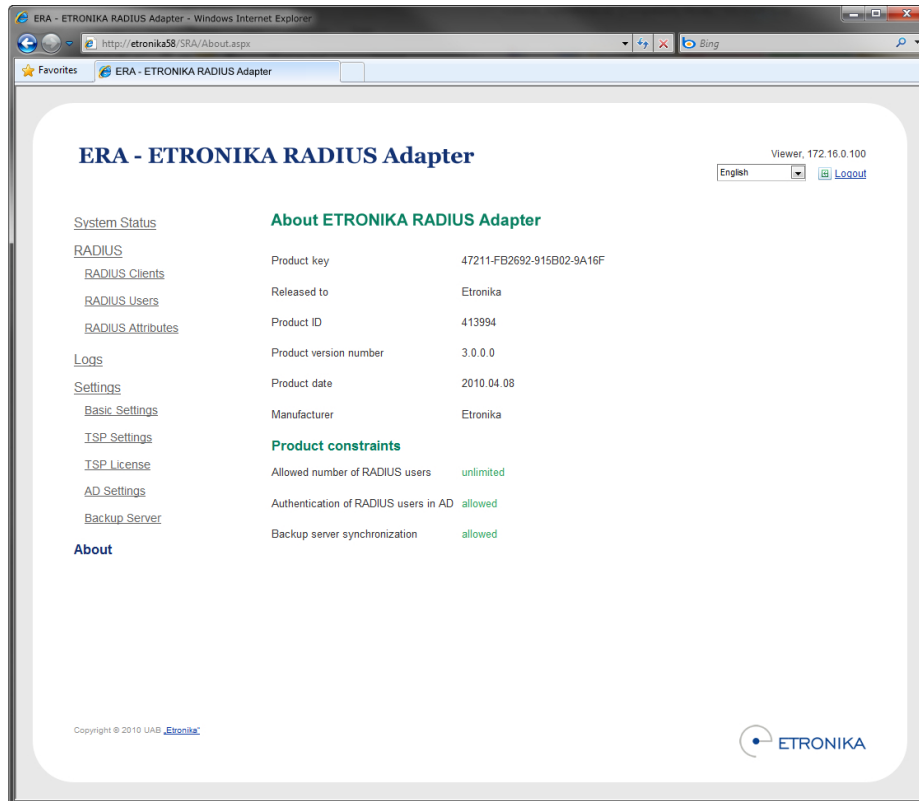
Why It's Better

Applicable both for small and enterprise businesses

Applicable both for small and enterprise businesses that have limited IT resources, but aim to guarantee high-level networking security.

Flexibility of ETRONIKA RADIUS Adapter allows adding as much users and applications as required.

How ERA Works?

Server Side

There are three components of Etronika RADIUS Adapter at the **server side**:

- **Administration Module**

- **Authentication Module**

- **ERA Users Database**

Server Side

Administration module

Administration module is Web application with Administration console that administers and manages backend processes. It administers user authentication policies. Its main blocks are:

- Management of the RADIUS clients (firewalls, NAS servers, etc.)

- Management of the users who can authenticate themselves via RADIUS protocol

- Management of the system security provisions

- System status information page

- Configuration of mobile signature provider

Server Side

Authentication module

Authentication module is extension of the RADIUS server that recognizes RADIUS users, searching for them in Active Directory or ERA Database. If user's identification through mobile signature is successful, the authentication module calls Web Service that authenticates user via ERA service.

Database

Database is an encrypted database where operational data are stored.
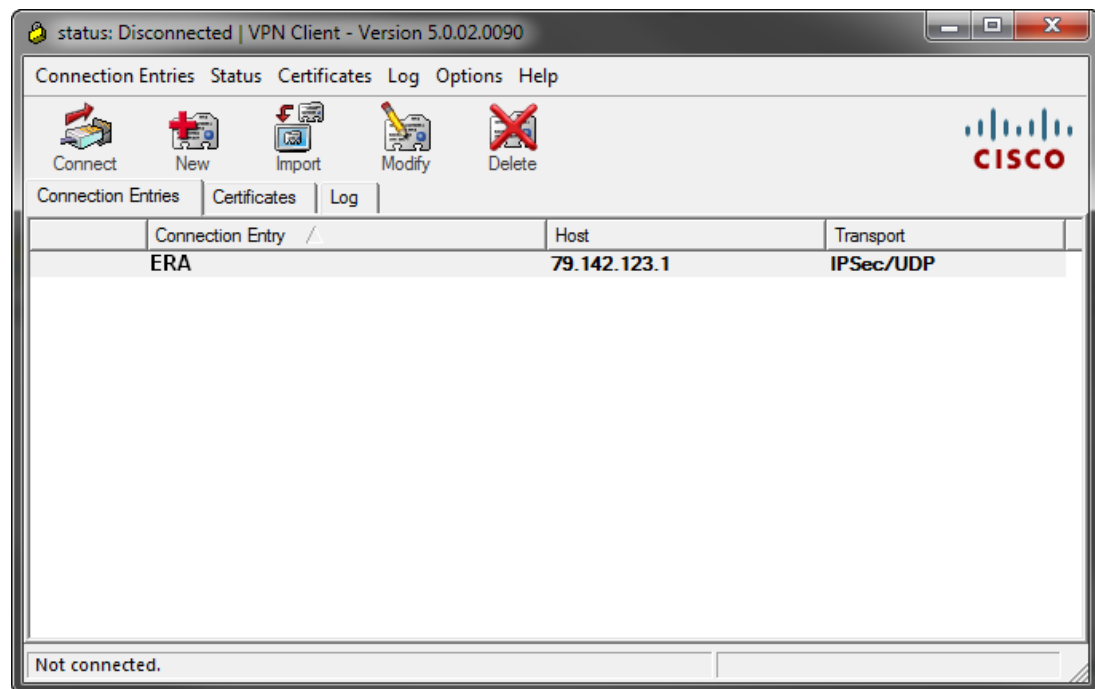
Standard ERA Setup
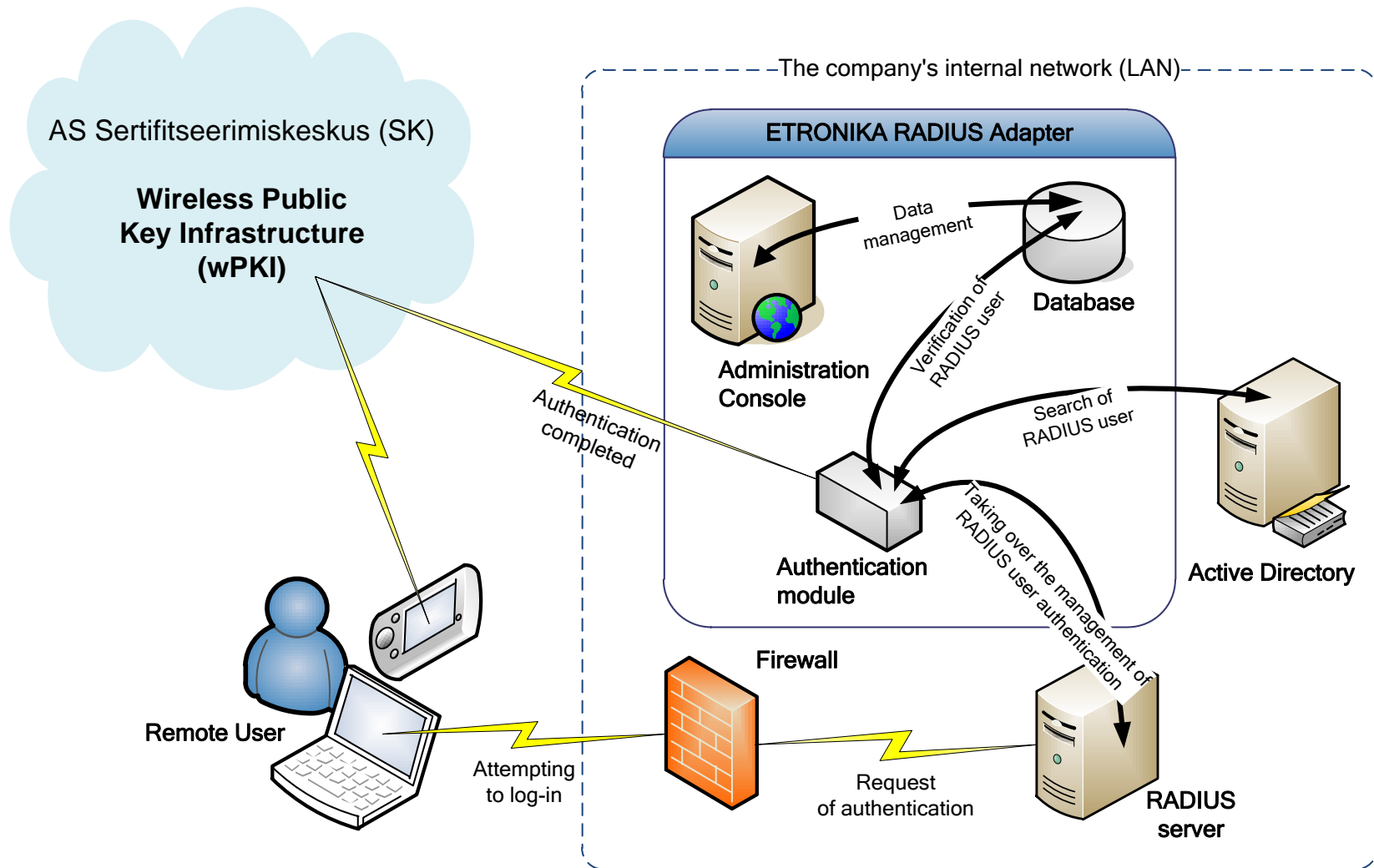
User Side

To login with a secure access the remote user needs:

- Individually owned **mobile signature** and **mobile phone**

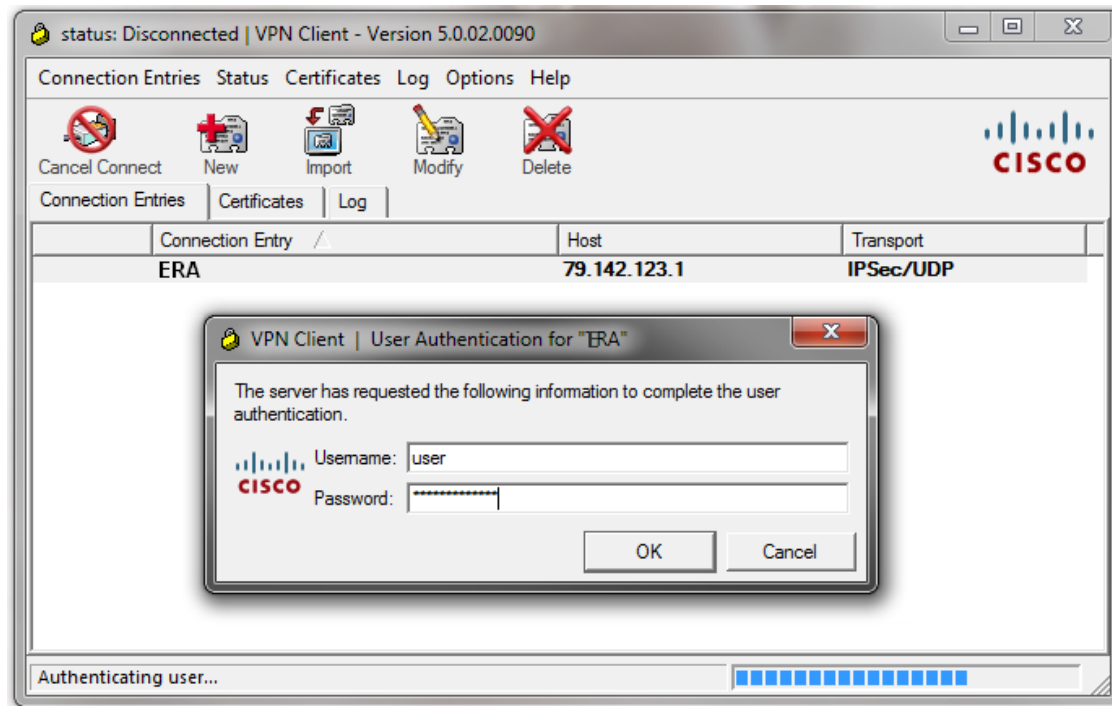- Assigned **VNP connection** client with added **ERA** connection **entry**

User Side

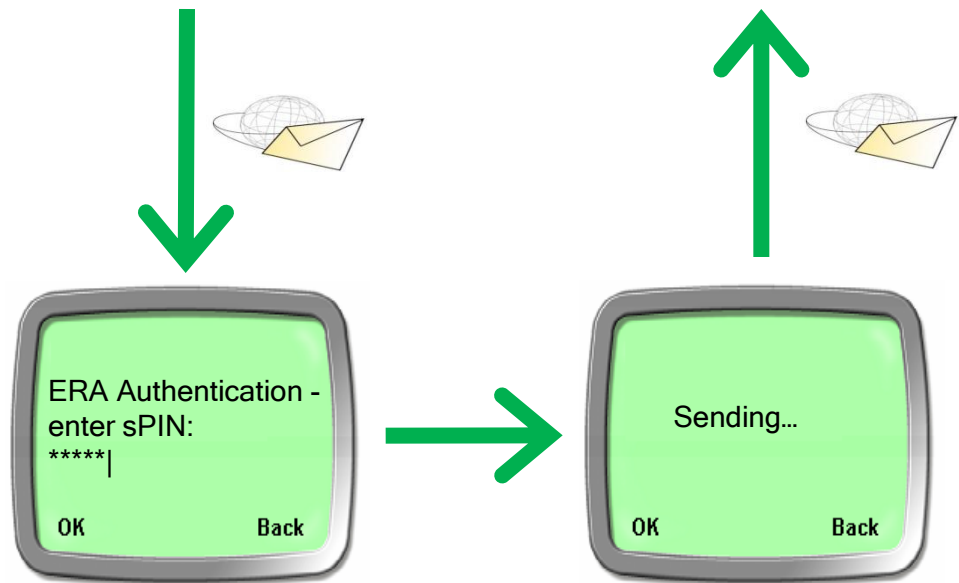1. **User opens VPN connection and clicks on ERA connection entry**

User Side

2. User enters his/her username and password

User Side

3. User receives message to his/her mobile phone asking to enter the sPIN of mobile signature

ERA Authentication -
enter sPIN:
*****|

OK   Back

Sending...

OK   Back

User Side

4. User enters the sPIN. The system identifies user, authorizes the VPN connection, and grants access to remote system or application.

Technical Requirements

Technical requirements for the Etronika RADIUS Adapter environment:

- Windows 2003/2008 Server

- NAS/IAS

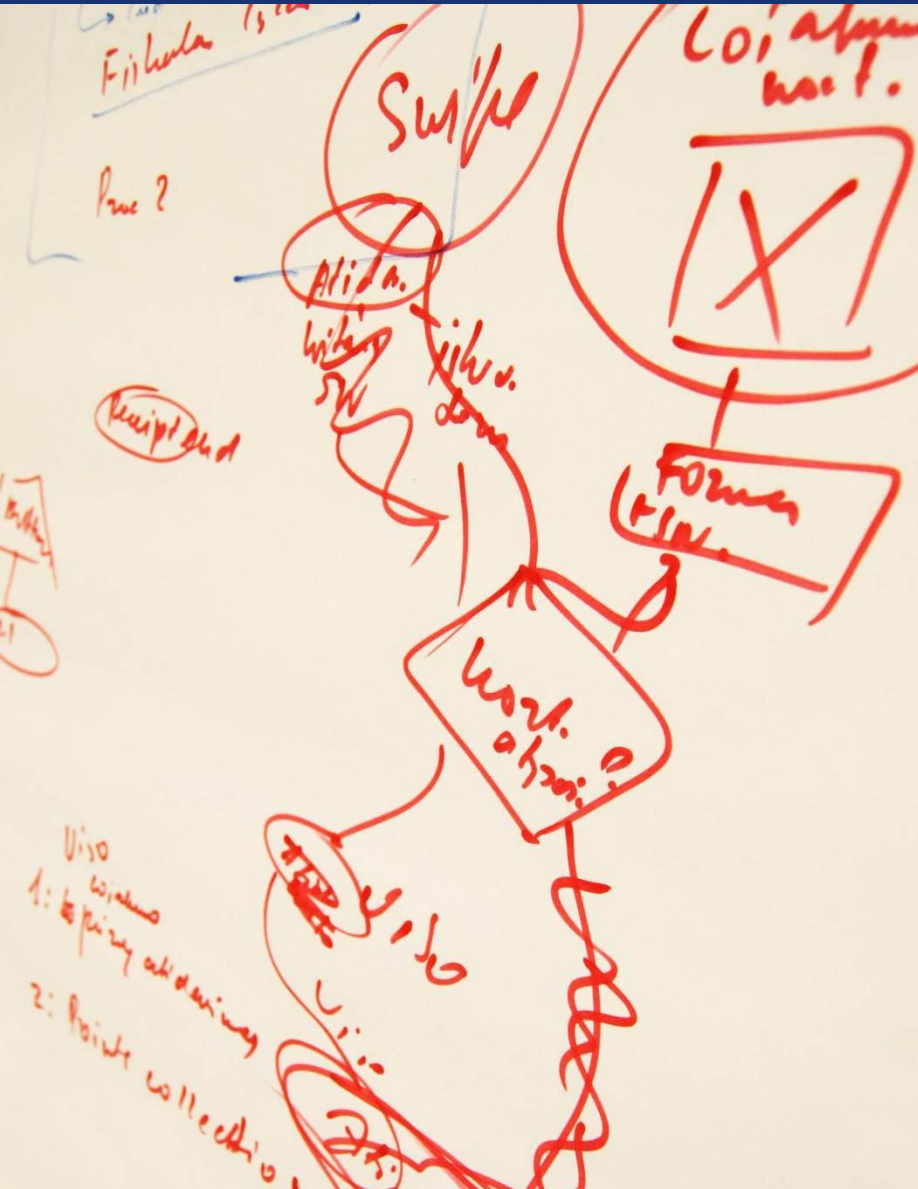- .NET Framework v.3.5

- IIS v.6 and higher

About ETRONIKA

Main Facts

- Established in year 2000, headquatered in Vilnius

- 30 employees (September, 2010)

- Highly skilled, certified professionals

- Awarded products

- Technology partners: Microsoft, IBM, Oracle, Vasco Data Security

E-Signature Competence

Since establishment ETRONIKA actively participates in security, cryptography and e-signature projects, thus promoting wireless PKI based digital signature usage.

According to TeliaSonera we were the first in the world to introduce mobile signature commercial pilot in e-banking in year 2005.