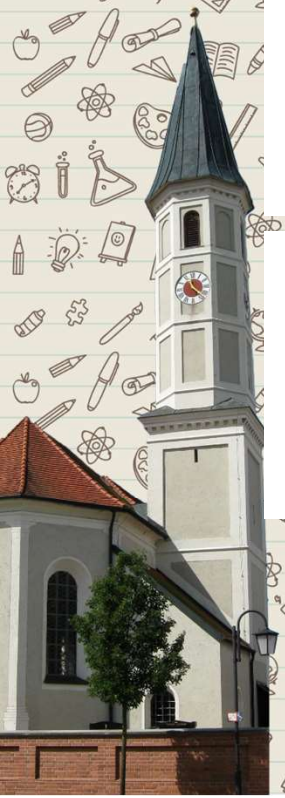
Clientless SSO for BYOD and unsupported/unmanaged platforms

TTP EMEA 2025

Václav Šamša, TDP



Introduction

- Authenticated – what next – session reminder:
  - Authentication factors/methods
  - Authorization user specific/not specific
- What are the options to authenticate the user and provide SSO without a client?
- Users are using:
  - VPN
  - Wifi

VPN & Wifi

- VPN authentication is usually 2FA nowadays
- Wifi authentication is usually 1FA but can be extended by smart approach
- There is a box or a virtualized box, firewall, wifi central etc, and that box knows who is the user, what is the matching object in some direktory, if the user is still connected and active or not
- 99% of boxes speak esperanto – Radius Accounting

What is RADIUS?

- RADIUS stands for **R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice
- It is a client-server protocol, established in early 90's
- It is de facto an industry standard, refer to RFC 2865
- Commonly used by leading networking product companies
- Client is a **N**etwork **A**ccess **S**erver, that queries the authentication server to get authentication, authorization and configuration for remote user
- **IMPORTANT – it has nothing with Radius Accounting !!**

What is RADIUS Accounting?

- It has nothing with RADIUS now. The primary purpose was to bill the client accordingly regardless the way the client got authenticated
- Network appliance can support RADIUS Accounting even if it doesn‘t support RADIUS Authentication
- Protocol works with 3 basic stones:
  - Accounting Start
  - Accounting Stop
  - Interim Update

What is RADIUS Accounting?

- Packets are protected with a pre-shared secret by MD5 hashing
- There are doubts about security but not in your server room
- Packets contain standard and Vendor Specific Attributes
- Important for us are:
  - Username
  - IP address assigned
  - Group membership
- Plus if it is a Start or Stop or Interim Update Packet

What kind of device my NAS can be?

- Generally speaking, user goes through NAS
- Very common NAS devices now are
  - Firewalls providing VPN
  - Cloud firewalls provided (yes, it works with cloud VPN)
  - Wifi access points or structures
  - Cloud Wifi control providers (yes, also)
- Less common NAS devices now are
  - Modem pools

What kind of device the user can use?

- Anything that can authenticate through the NAS
- Boring but working are Windows, MacOSX, Linux
- BYOD (above plus mobiles) and devices like ChromeBooks, various PADs etc
- While SAML, JWT, and OpenAuth work with a single browser, RADIUS Accounting works with the user‘s identity behind the IP address the device has assigned at the moment

WiFi Access Point as NAS

VPN (FireWall) as NAS

RADIUS Accounting server?

- It can be any device supporting the server side role
- Some devices can work as a client and as a server at the same time
- For example – once user authenticates with Chromebook to WiFi network, WiFi AP can send RADIUS Accounting packet to Firewall to open also the way out, to the internet
- RADIUS Accounting packet can contain group membership info to instruct the Firewall where the user can go

VPN as RADIUS Accounting server example

IPSEC

Group

Username/Password

FireWall

VPN Authentication quality

- Common implementation works with IPSEC:
  - Group Authentication with pre-shared pfc profile includes identity check of the firewall
  - User Authentication with username and password (or certificate) provided by user. Username/Password against LDAP
- This authenticaton is widely accepted as a two factor authentication (group and user)
- VPN authentication is (and must be ☺) very secure

The role of KeyShield SSO

- KeyShield SSO can serve as many RADIUS Accounting clients
- Each client instance can inform different RADIUS Accounting server about the user‘s identity, IP address and status
- Once the user gets authenticated from Windows Workstation for example, KeyShield SSO can inform the firewall, proxy or webcontent manager about the user‘s identity, IP address and group membership
- User can go out to the internet after Start packet and the way out is closed after the Stop packet.

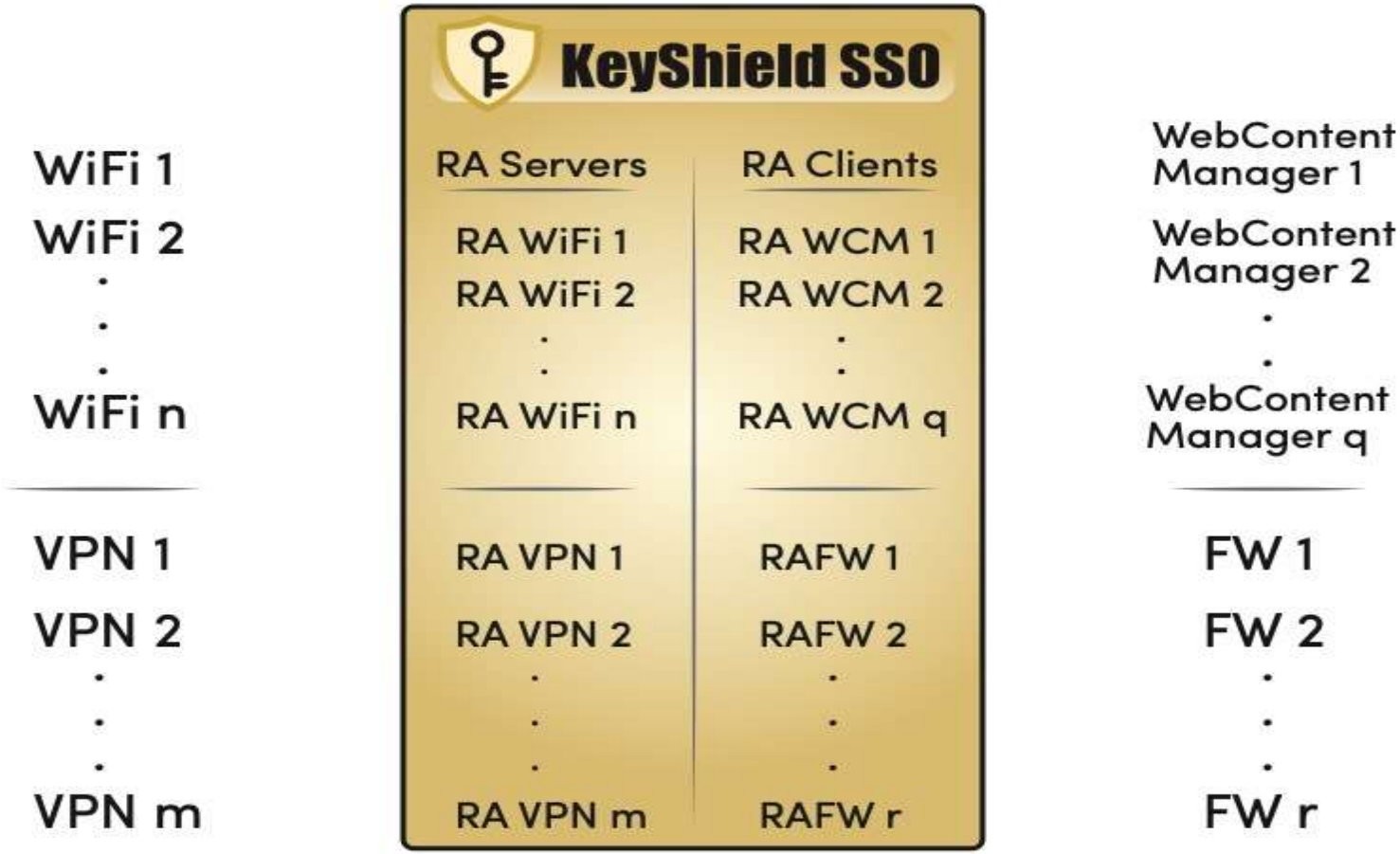
KeyShield SSO bonus - dynamic group membership

- KeyShield SSO can map LDAP groups to RADIUS Accounting groups with a static map table
- But KeyShield SSO can work with dynamic groups also:
  - Teacher can assign the dynamic group to the whole classroom or class to block access completely
  - Or to let students work with the online test but not with google
  - Or to let them go anywhere (except ugly sites, of course)
- Controlled by KeyShield SSO, provided by firewall, proxy or web-content manager

The role of KeyShield SSO cont.

- KeyShield SSO can serve as many RADIUS Accounting servers
- Each server instance can receive information from different RADIUS Accounting client
- Once the user gets authenticated to VPN for example, the firewall informs KeyShield SSO about the user‘s identity and IP address
- Start Accounting is login, Interim Update keeps the user logged in, and Stop Accounting logs out the user

The role of KeyShield SSO – can be complex



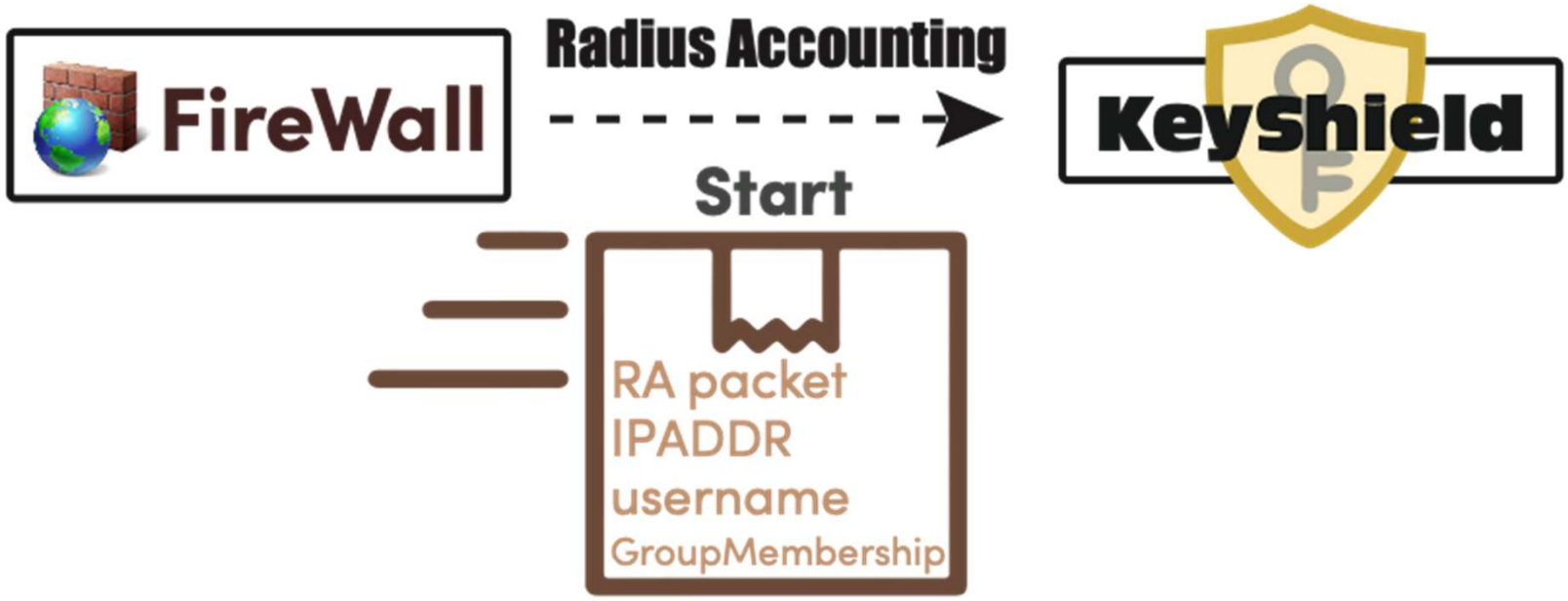
WiFi 1
WiFi 2
.
.
.
WiFi n

VPN 1
VPN 2
.
.
.
VPN m

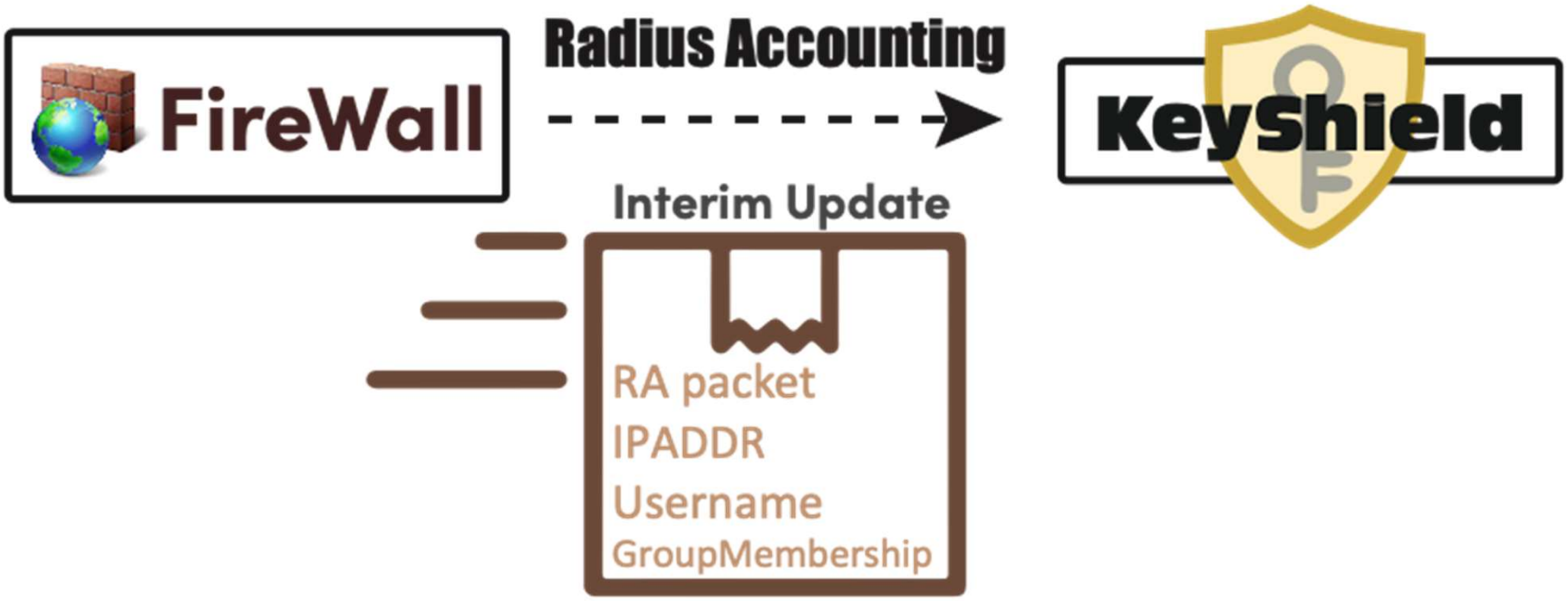
WebContent Manager 1
WebContent Manager 2
.
.
WebContent Manager q

FW 1
FW 2
.
.
.
FW r

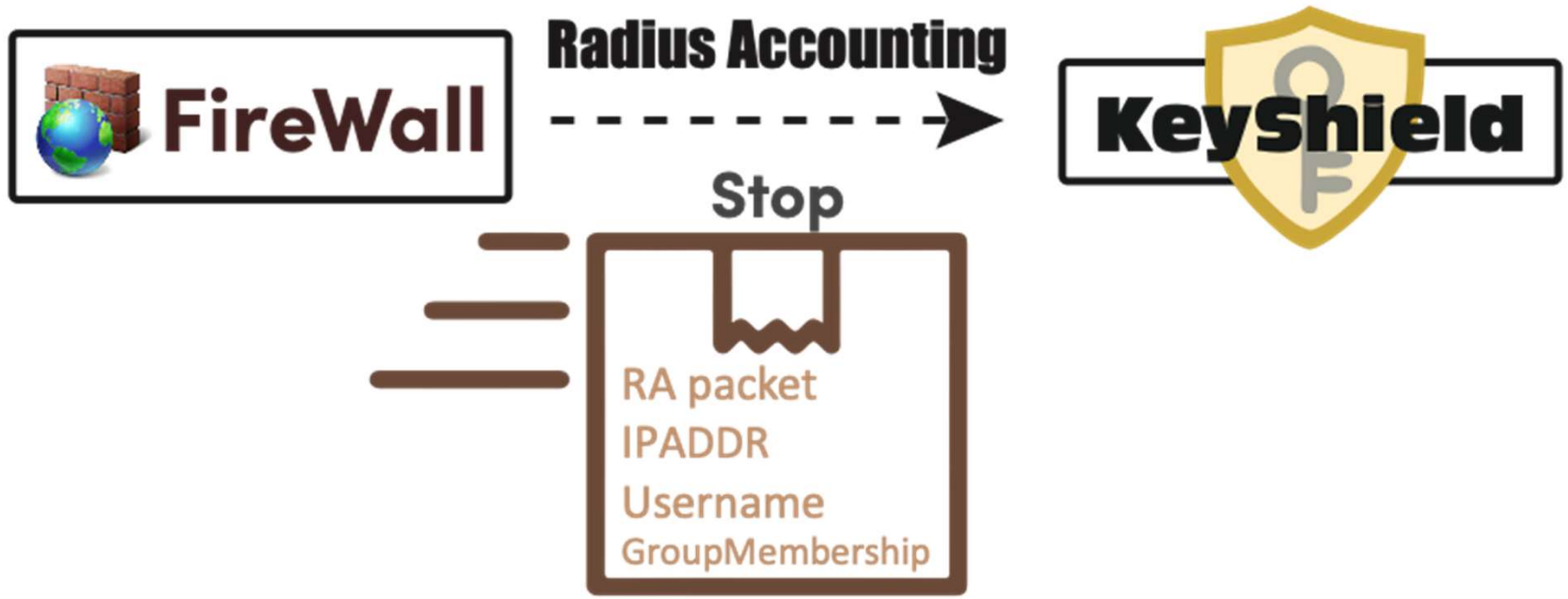
KeyShield SSO as RADIUS Accounting server



KeyShield SSO as RADIUS Accounting server



KeyShield SSO as RADIUS Accounting server



KeyShield SSO client ver RADIUS Accounting auth

- KeyShield SSO client and server check together if the user‘s IP address is unique from the server‘s point of view
- This works with RADIUS Accounting authentication to KeyShield SSO server similarly
- If the client communicates from the same IP address as reported – the address is OK, and the authentication is accepted
- RADIUS Accounting authentication can work with an unique IP address only

KeyShield SSO keeps a list of the authenticated users

KeyShield SSO

Authenticated users

Marc 192.168.10.33 1

Tony 192.168.10.34 2

.

.

.

Lea 192.168.10.41 9

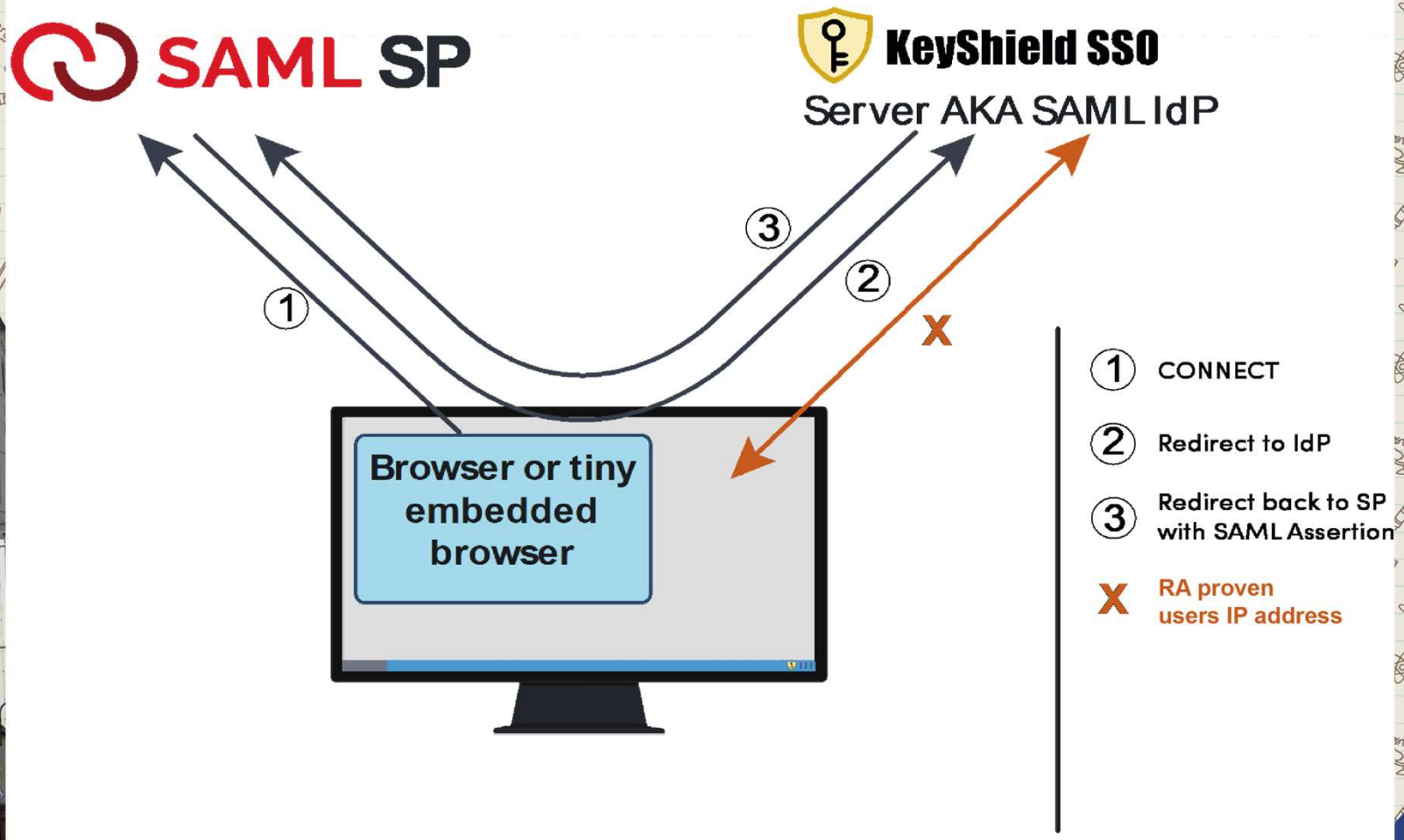
What the authenticated user can do?

- KeyShield SSO provides following options:
  - Direct unique IP address authentication – supported by many partners incl MicroFocus with FILR for example
  - SAML authentication with any browser or compatible app – this works with tons of SAML enabled onprem, hosted and cloud providers incl. Google, Microsoft etc
  - JWT authentication with any compatible app – this works with various email systems incl. Kerio for example
  - OIDC – the same

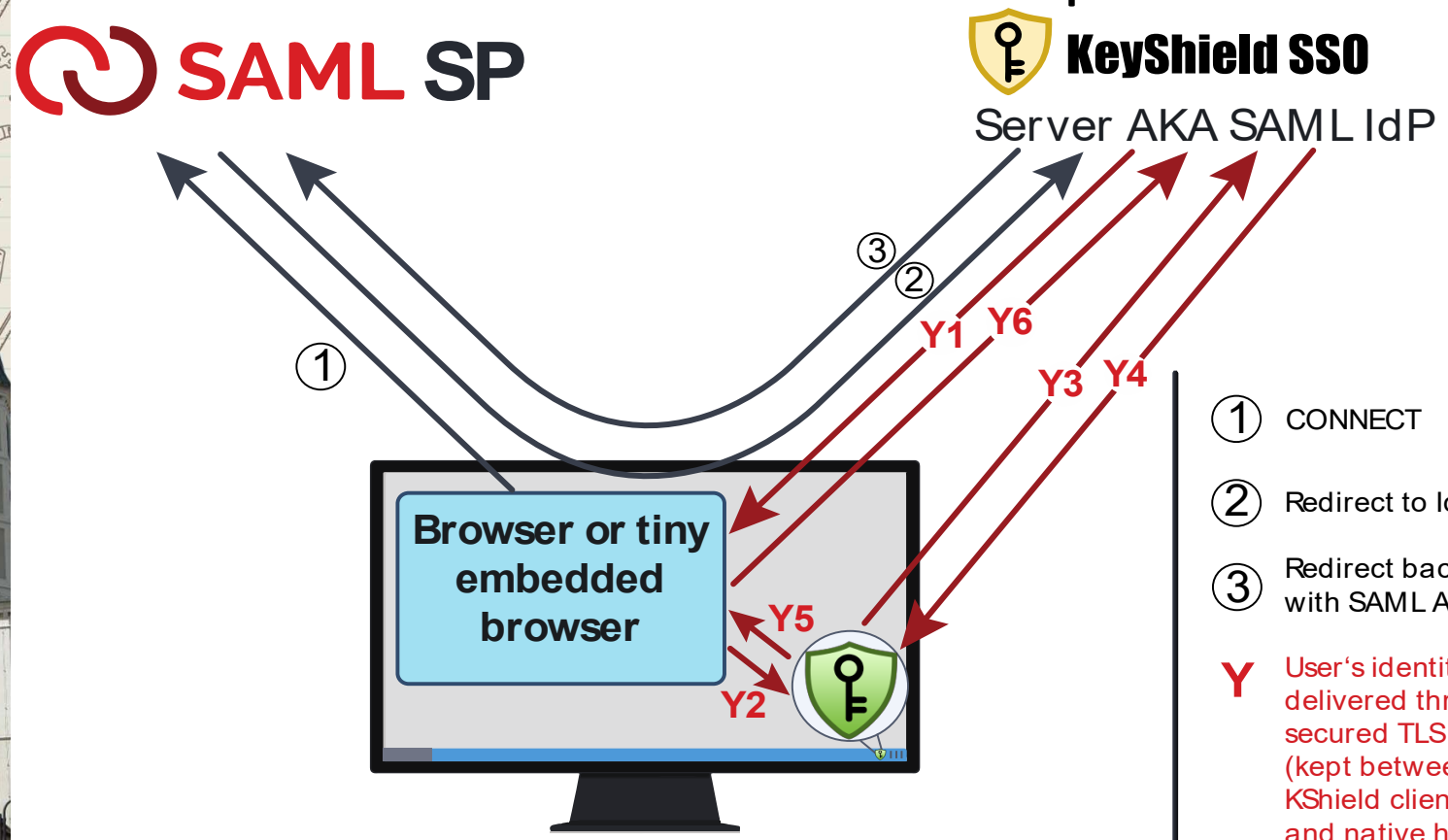
IP Address authentication hardening note

- KeyShield SSO 8.6 includes special option to make IP Address authentication more secure
- By default, KeyShield SSO checks the user‘s device every 2 mins
- With the hardening option active, user‘s device is checked for each auth request
- Implemented for NAS devices with suboptimal management of the pool of addresses

How SAML authentication works?



SAML with token for comparison?



① CONNECT

② Redirect to IdP

③ Redirect back to SP with SAML Assertion

Y User's identity token delivered through secured TLS channel (kept between KShield client & server) and native host

Why this session?

- RADIUS Accounting is very flexible – whoever and whatever can authenticate to your WiFi or VPN or so can enjoy SSO to on-prem, hosted or cloud Services
- This authentication can be seamless, not abusing, causing no delays - also because KeyShield SSO is at least 60 times faster than anything else (not kidding, 60x)
- Authentication is great for statistics
- Authentication is a must for monitoring

Why this session? Cont.

- Monitoring doesn‘t sound such academic in terms of freedom
- But it is more and more required by law
- Or required by internal school rules
- Or the age of the user is the driving information:
  - Teenagers and kids are not allowed to watch anything. It‘s a law.
  - Adults can sign a statement, that they do not want to be protected
- If your users/guests/whoever are authenticating with their accounts now to use Wifi, VPN, internet or so, you can start using RADIUS Accounting without any changes. Seamlessly!

Q & A

(FoC during TTP)

TTP EMEA 2025

Václav Šamša, **TDP**