

Modern RDP security

Ing. Ondřej Ševeček | GOPAS a.s. |
MCSM:Directory | MVP:Enterprise Security | CEH | CHFI | CISA |
ondrej@sevecek.com | www.sevecek.com |



PLATINUM PARTNER



GOLD PARTNER

DEVCON HALL SHOWIT HALL



SILVER PARTNER

PROFINIT
NÁSKOK DÍKY ZNALOSTEM

GENERAL PARTNER



moje kurzy v GOPASu

GLAB007 - capture the flag 1 - hackni si podnikovou síť
GLAB008 - capture the flag 2 - hackni si podnikovou síť
GOC175 - implementace bezpečnosti
GOC169 - ISO 27001
GOC172 - Kerberos troubleshooting

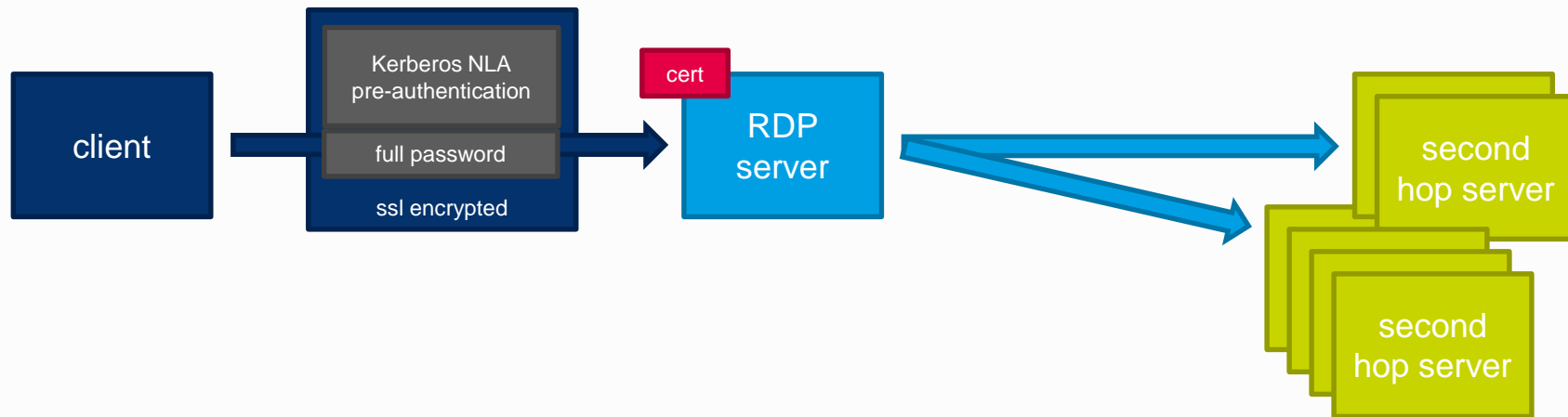
Agenda

- Password transport in full
- SSO principles
- Channel encryption with SSL/Kerberos/NLA
- User access to secure RDP servers
- Admin access to insecure endpoints

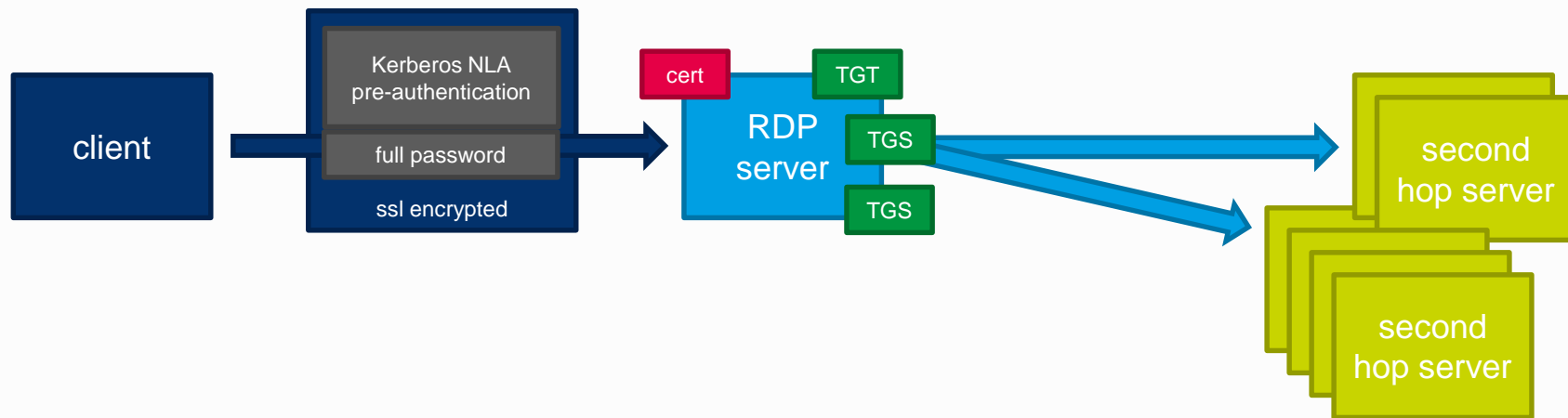
The problem

- **clean** password transport by default to enable SSO
 - SSL encrypted?!
 - transport **on all versions**, in-memory permanently until 2012 R2 and Windows 8.1
- compare with Enter-PSSession
 - double-hop authentication
 - Get-WSManCredSSP
 - Enable-WSManCredSSP -Role Client -DelegateComp
 - Enable-WSManCredSSP -Role Server
 - Enter-PSSession -Authentication CredSSP -Credential (Get-Credential)

The default scenario



The default scenario



Transport protection

- never ever skip **warnings!**
- verify lock icon!
 - NLA
 - valid SSL certificate on non-Kerberos scenarios
 - Kerberos authentication
 - or **both**
 - servicePrincipalName: TERMSRV/rdp.gopas.cz

Require server authentication on clients

Sec: RDP Client Require Server Authentication		show all
Data collected on: 13.05.2019 12:06:08		
General		show
Computer Configuration (Enabled)		hide
Policies		hide
Administrative Templates		hide
Policy definitions (ADMX files) retrieved from the central store.		
Windows Components/Remote Desktop Services/Remote Desktop Connection Client		hide
Policy	Setting	Comment
Configure server authentication for client	Enabled	
Authentication setting:		Do not connect if authentication fails

Two scenarios

- user access
 - limited user works on a secure server
- admin access
 - powerful privileged admin connects to insecure machines

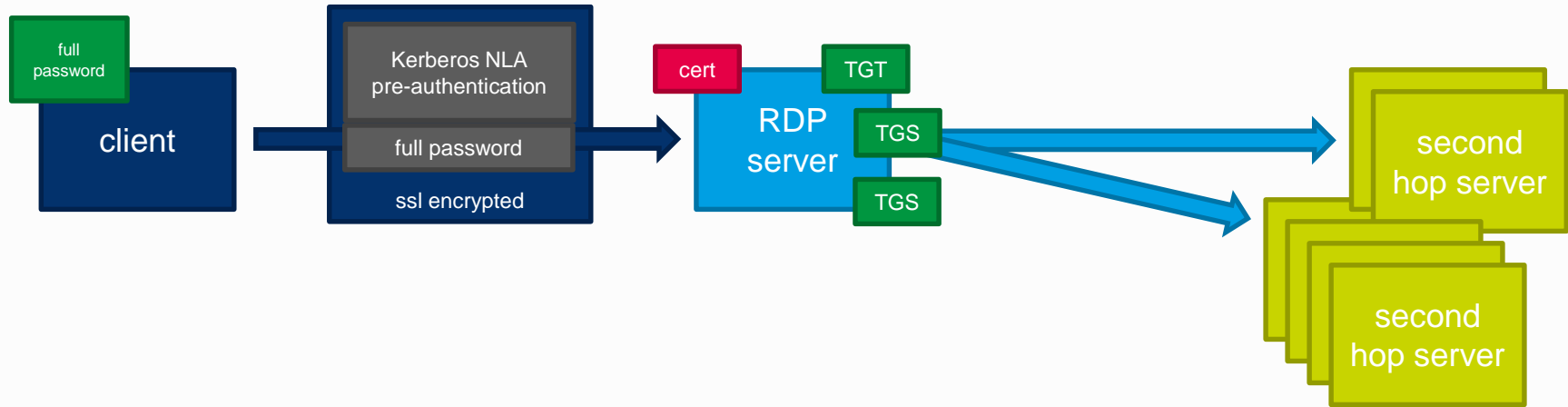
User access

- limit password exposure
 - RDP SSO since Windows Vista/7/2008
 - prevent saving passwords
- never send clean password
 - /remoteGuard since Windows 10/2016
 - does **not** need Credentials Guard enabled on either side

Deny saving RDP passwords on clients

Computer Configuration (Enabled)			hide
Policies			hide
Windows Settings			hide
Security Settings			hide
Local Policies/Security Options			hide
Network Access			hide
Policy	Setting		
Network access: Do not allow storage of passwords and credentials for network authentication	Enabled		
Administrative Templates			hide
Policy definitions (ADMX files) retrieved from the central store.			
Windows Components/Remote Desktop Services/Remote Desktop Connection Client			hide
Policy	Setting	Comment	
Do not allow passwords to be saved	Enabled		

RDP SSO for limited users (2012R2/8.1 and older)



Client RDP SSO settings for standard users (2008/Vista/7+)

Allow delegating default credentials

Allow delegating default credentials

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Options:

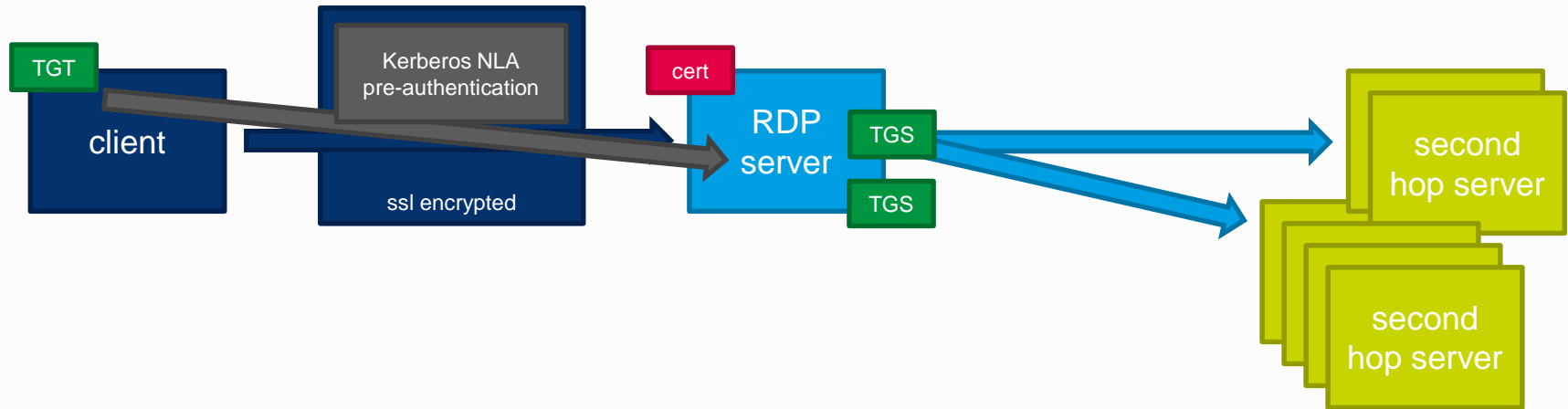
Add servers to the list:

	Value
▶	TERMSRV/rdp.gopas.cz
•	

Add servers to the list

Concatenate

Remote Guard for limited users (2016/10 and newer)



RemoteGuard requirements

- Kerberos server authentication + Kerberos user NLA authentication
- Windows 10.1607+, Windows 2016+
- HKLM\System\CurrentControlSet\Control\LSA
 - DisableRestrictedAdmin = DWORD = 0
 - must be enabled on the **remote RDP server**
- /remoteGuard cmd switch **requires Administrators** membership
 - user get "The requested session access is denied" for non-Administrators
- use GPO **client** enforcement for **non-Administrators**

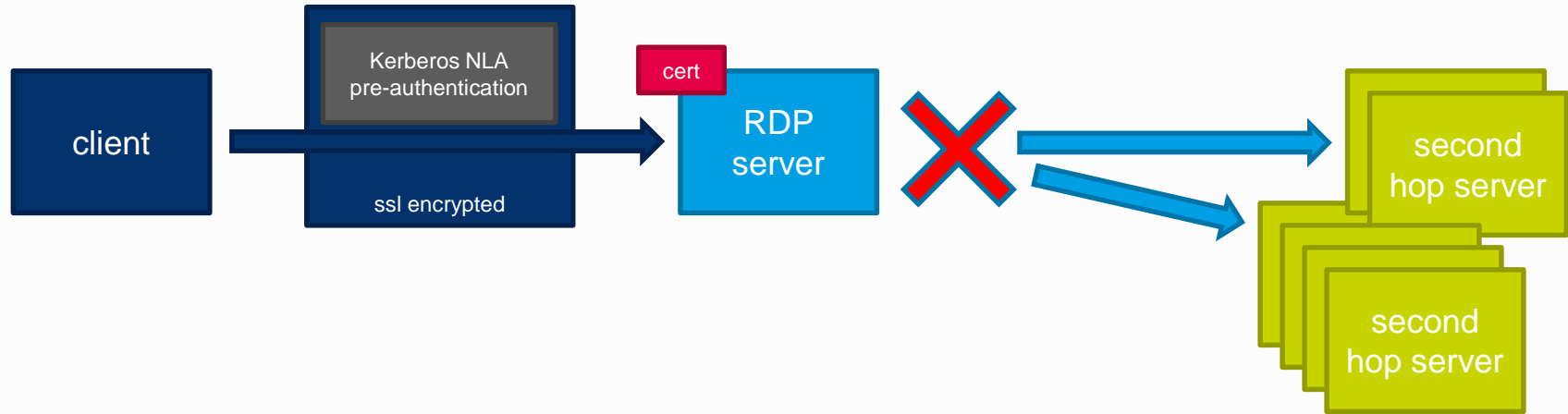
Enforce RemoteGuard on **clients** with GPO for non-Administrators

The screenshot shows the 'Restrict delegation of credentials to remote servers' GPO configuration window. The window title is 'Restrict delegation of credentials to remote servers'. The main content area has a header with the same title and two buttons: 'Previous Setting' and 'Next Setting'. Below the header, there are three radio button options: 'Not Configured', 'Enabled' (which is selected), and 'Disabled'. To the right of these options is a 'Comment:' text box. Below the radio buttons is a 'Supported on:' section with a text box containing 'At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1'. At the bottom, there are two sections: 'Options:' and 'Help:'. The 'Options:' section contains a dropdown menu labeled 'Use the following restricted mode:' with 'Require Remote Credential Guard' selected. The 'Help:' section contains a text box with the following text: 'When running in Restricted Admin or Remote Credential Guard mode, participating apps do not expose signed in or supplied credentials to a remote host. Restricted Admin limits access to resources located on other servers or networks from the remote host because credentials are not delegated. Remote Credential Guard does not limit access to resources because it redirects all requests back to the client device.'

Admin access

- /restrictedAdmin
 - since 2012 R2/8.1
 - since 7/2008 R2 with update
- HKLM\System\CurrentControlSet\Control\LSA
 - DisableRestrictedAdmin = DWORD = 0

Restricted Admin mode (Windows 2012 R2/8.1 and update for 2008 R2/7 and newer)



Enforce restricted admin

- GPO forcing admin clients to use /restrictedAdmin
- Authentication policies
 - client with NLA
 - server even without NLA
 - Windows 2008R2/7 blocked by default

Děkuji za pozornost

moje kurzy v GOPASu

GLAB007 - capture the flag 1 - hackni si podnikovou síť

GLAB008 - capture the flag 2 - hackni si podnikovou síť

GOC175 - implementace bezpečnosti

GOC169 - ISO 27001

GOC172 - Kerberos troubleshooting

www.gopas.cz