Deep Dive :

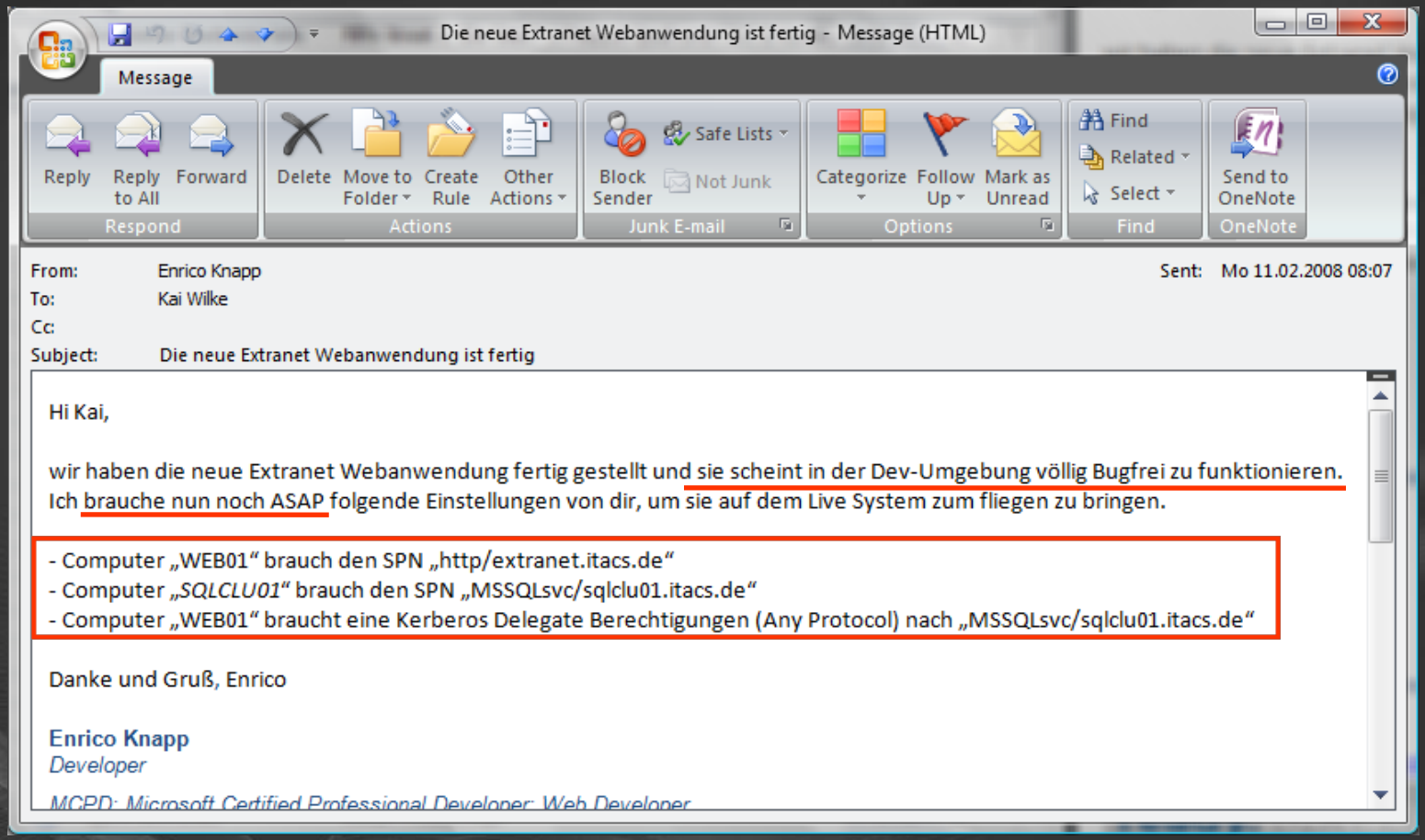
Kerberos, Protocol Transition und Constrained Delegation

Kai Wilke
Consultant IT-Security
MVP ISA Server und Security (a.D.)
ITaCS GmbH
mailto:kw@itacs.de

Was ist überhaupt Kerberos?

- „Cerberus“ war ein dreiköpfiger Wachhund vor den Toren Hades
  - 1. Kopf = Client Principal
  - 2. Kopf = Service Principal
  - 3. Kopf = Kerberos Dienste
- In der Netzwerkwelt ist es ein de facto Standard
  - Entwickelt vom MIT und in RFC 1510 niedergeschrieben
  - Bietet leistungsfähige, sichere und hetrogene Authentifizierung
  - Kerberos V5 ermöglicht eine Federation und Delegation
- Im AD ist Kerberos das primäre Anmeldeprotokoll
  - LM und NTLM (v1/v2) sind nur noch legacy Protokolle
  - Es ist einfach da und muss wenig beachtet werden...

Wenn Entwickler mir Emails zusenden …

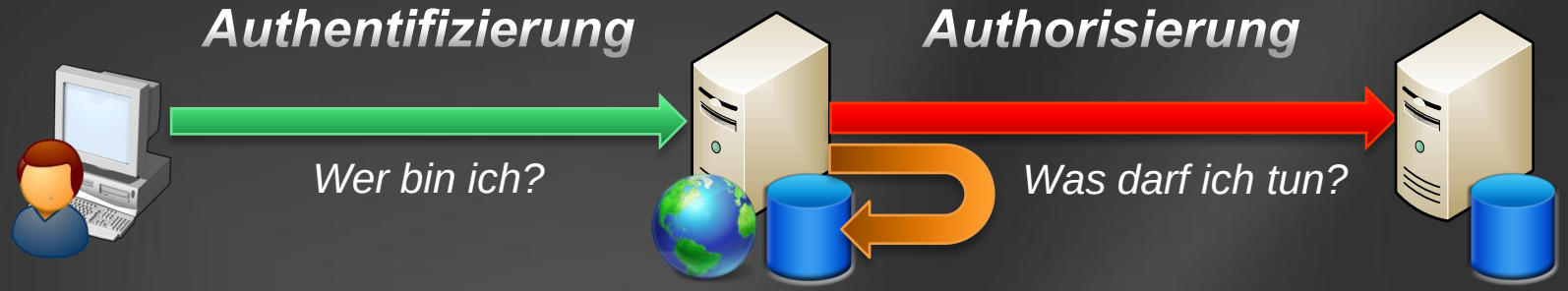


…, dann hinterfrage ich viele Details!

Agenda

- 1x1 der Authentifizierung und Authorisierung
  - Trusted Subsystem vs. Impersonation Model
  - Prozesskonten und Zugriffe auf Ressourcen
- Deep Dive in das Kerberos Protokoll
  - Authentifizierung und Zugriffe auf Ressourcen
  - Kerberos Service Principal Names (SPNs)
  - Kerberos Delegation und W2K3 Extensions
    - Kerberos Constrained Delegation (A2D2)
    - Kerberos Protocol Transition (T2A4D)
- Zusammenfassung und Ressourcen

Authentifizierung und Authorisierung

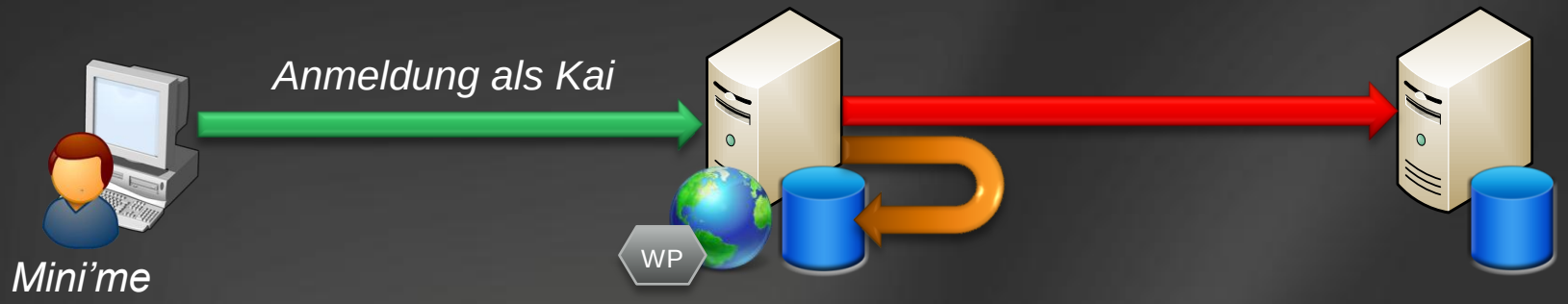


- Im Falle des „Trusted Subsystems“
  - Die Anwendung steuert die Authorisierung der Benutzer.
  - Auf Ressourcen wird hierbei mit der Prozess-Identität der Anwendung zugegriffen.
- Im Falle des „Impersonation Models“
  - Die Anwendung impersoniert den Benutzer und die Ressource steuert eigenständig die Authorisierung.
  - Lokale Zugriffe (Impersonation) und Remote-Zugriffe (Delegation).

Trusted Subsystem vs. Impersonation Model

- Trusted Subsystem
  - Anwendung verwendet eine feste Identität
  - Anwendung kann die Authentifizierung steuern
  - Anwendung muss die Authorisierung und das Auditing steuern
  - Hohe Performance durch Connection Pooling zu Backend-Servern
  - Verteilte Umgebungen benötigen keine AD-Mitgliedschaft
- Impersonation Model (Identification / Impersonation / Delegation)
  - Anwendung verwendet für Aktionen die Benutzeridentität
  - Native Authorisierung und Auditing an der Ziel-Ressource
  - Skalierung wird durch eine Vielzahl von Identitäten und Connections zu der Ressource beeinträchtigt
  - Delegierung der Authentifzierungsdaten zu den Backend-Servern
    - Kerberos als Authentifizierungs-Protokoll hierbei erforderlich

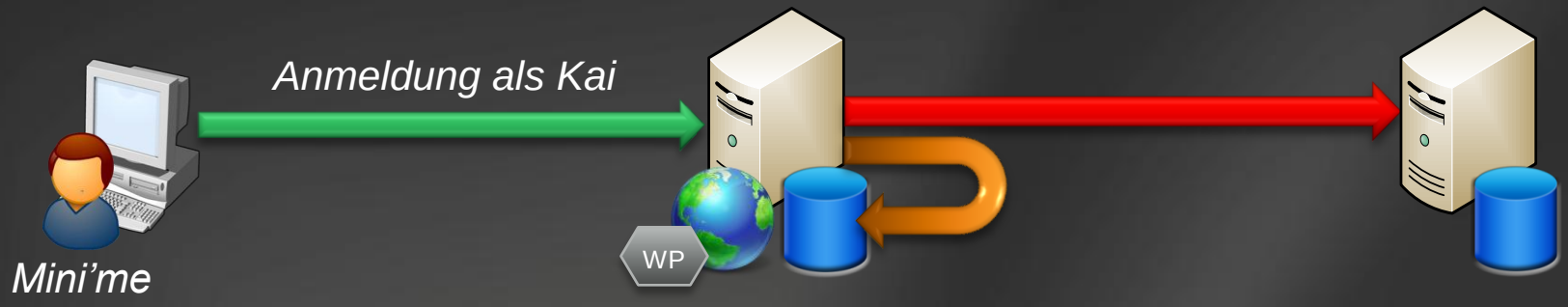
Prozesskonten und Zugriffe auf Ressourcen
Trusted Subsystem



Anwendungsidentität	Lokaler Zugriff	Remote Zugriff
Network Service	Network Service	APP1$
Local Service	Local Service	ANONYMOUS
Local System	SYSTEM	APP1$
Dom Account: WEB1	WEB1	WEB1

- Unbedingt den Domänennamen mit angeben (CONTOSO\WEB1)
- Pre2008: Das Domänenkonto sollte zur lokalen IIS Worker Process-Gruppe hinzugefügt werden (IIS_WPG)
- Win2008: Automatische Zuordnung über IIS_IUSR Gruppe

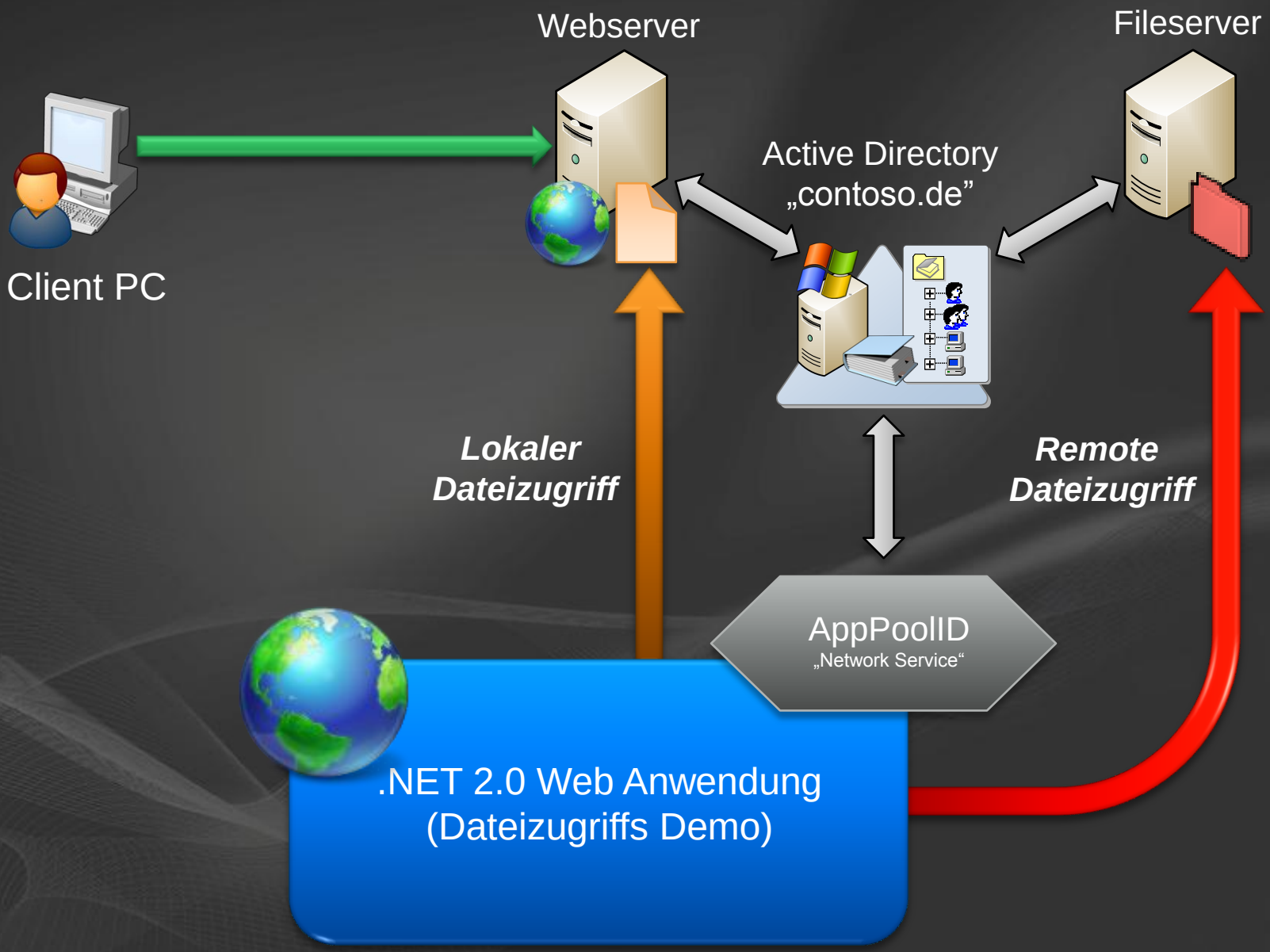
Prozesskonten und Zugriffe auf Ressourcen
Impersonation (ohne Delegation)



Anwendungsidentität	*Lokaler Zugriff*	*Remote Zugriff*
Network Service	Kai	ANONYMOUS
Local Service	Kai	ANONYMOUS
Local System	Kai	ANONYMOUS
Dom Account: WEB1	Kai	ANONYMOUS

- Lokal: Anwendungsidentität braucht „SeImpersonationPrivilege“
  - Konfigurierbares Systemrecht ab Windows 2000 SP4
- Remote: Kerberos Delegation wird benötigt, bevor Remote-Zugriffe ebenfalls Kais Identität verwenden können...

Demo Environment



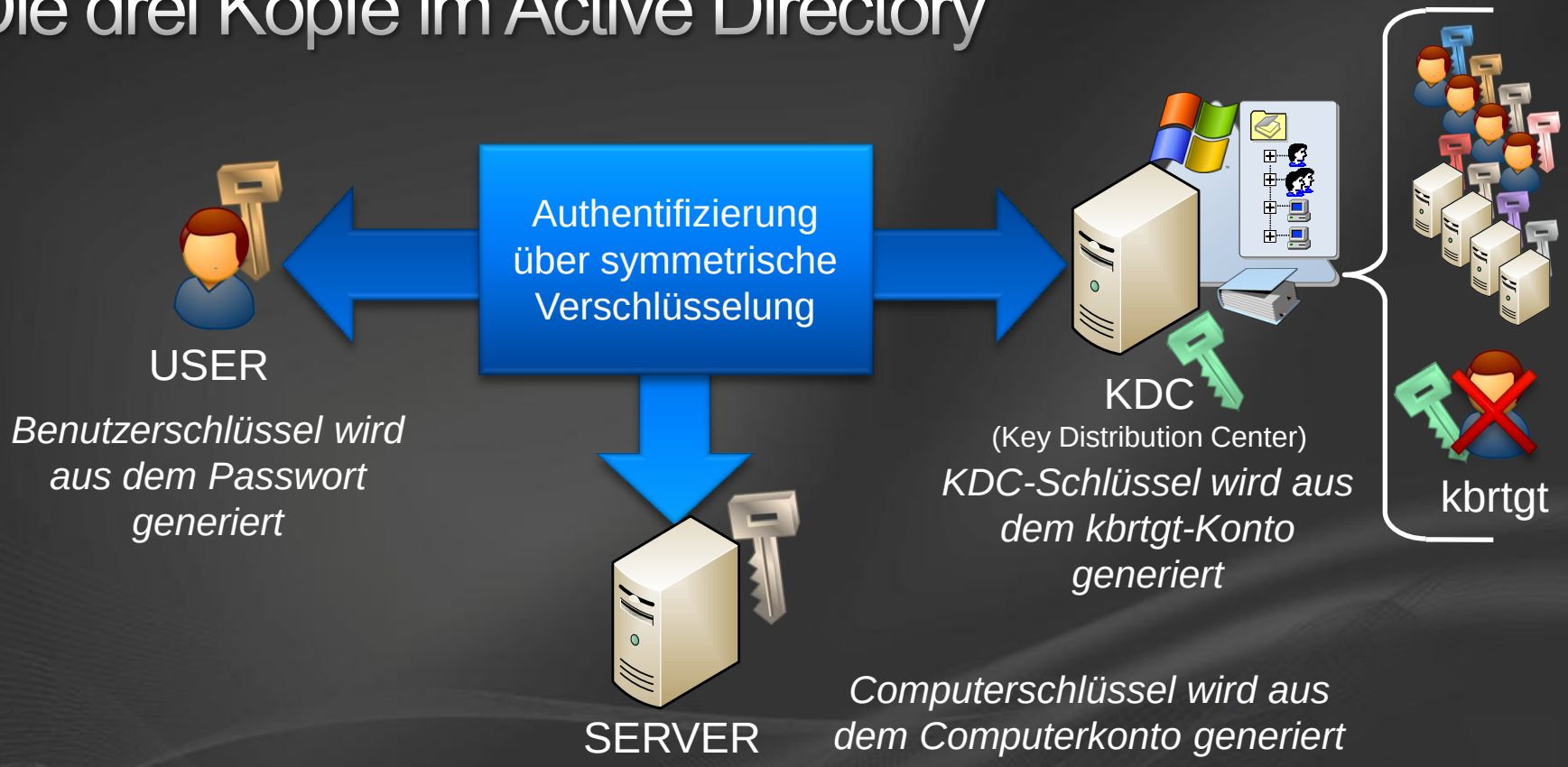
{ .Net Impersonation }

Kai Wilke
Consultant IT-Security
MVP ISA Server und Security (a.D.)
mailto:kw@itacs.de

Agenda

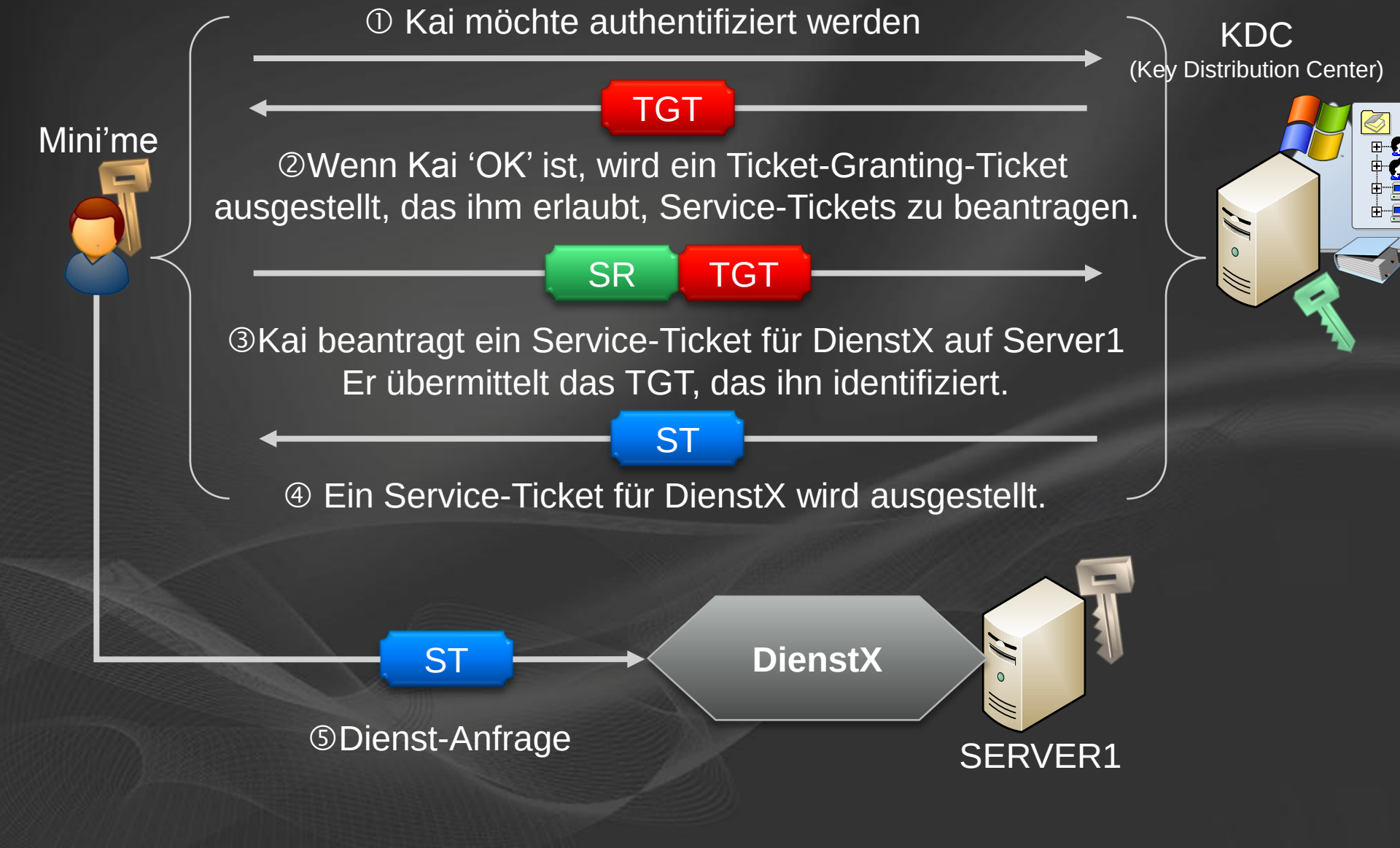
- 1x1 der Authentifizierung und Authorisierung
  - Trusted Subsystem vs. Impersonation Model
  - Prozesskonten und Zugriffe auf Ressourcen
- Deep Dive in das Kerberos Protokoll
  - Authentifizierung und Zugriffe auf Ressourcen
  - Kerberos Service Principal Names (SPNs)
  - Kerberos Delegation und W2K3 Extensions
    - Kerberos Constrained Delegation (A2D2)
    - Kerberos Protocol Transition (T2A4D)
- Zusammenfassung und Ressourcen

Funktionsweise von Kerberos
Die drei Köpfe im Active Directory



- Alle Köpfe sind Security Principals in der Kerberos Realm
- Um symmetrische Verschlüsselung nutzen zu können, müssen gemeinsame Geheimnisse vorhanden sein

Funktionsweise von Kerberos
Authentifizierung im Überblick



Funktionsweise von Kerberos
Kerberos Tickets

TGT

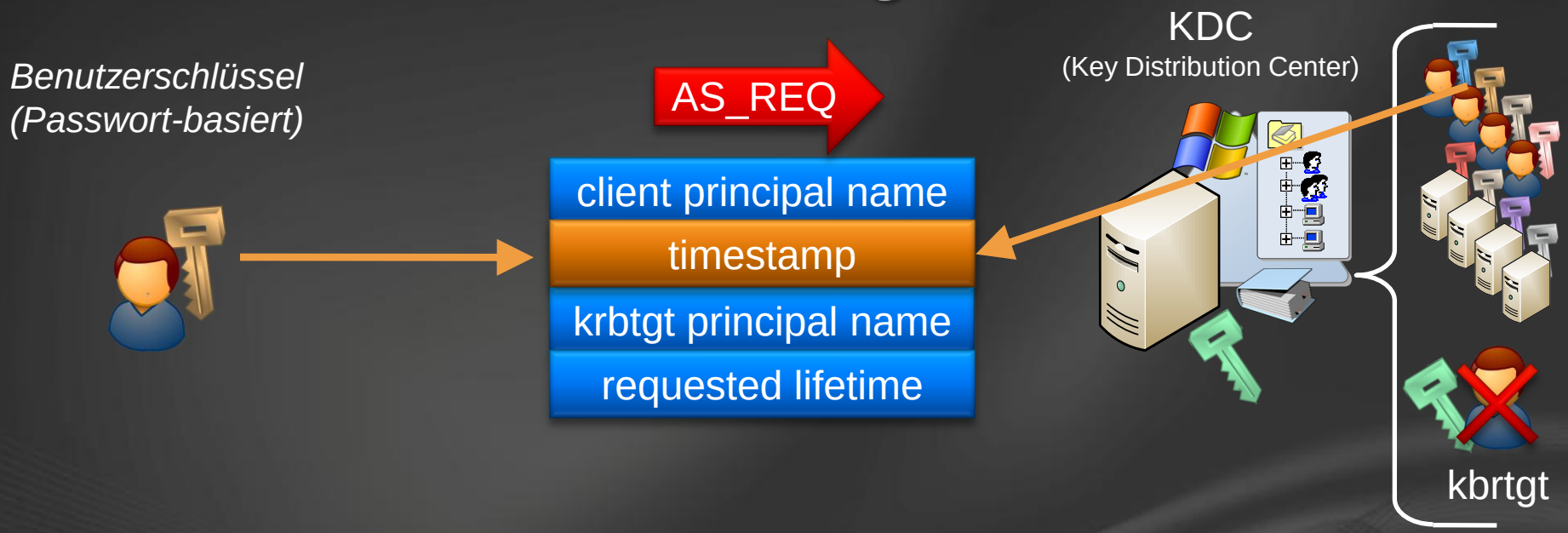
- Identifiziert den Benutzer gegenüber den KDCs bei späteren Service-Ticket-Anfragen
  - Macht spätere Re-Authentifizierungen unnötig

ST

- Nur gültig zwischen einem Benutzer und Dienst
  - Bietet gegenseitige Authentifizierung zwischen den beiden Security Principals
  - Beschleunigt den Sitzungsaufbau, da der Dienst nicht den Benutzer erneut authentifizieren muss

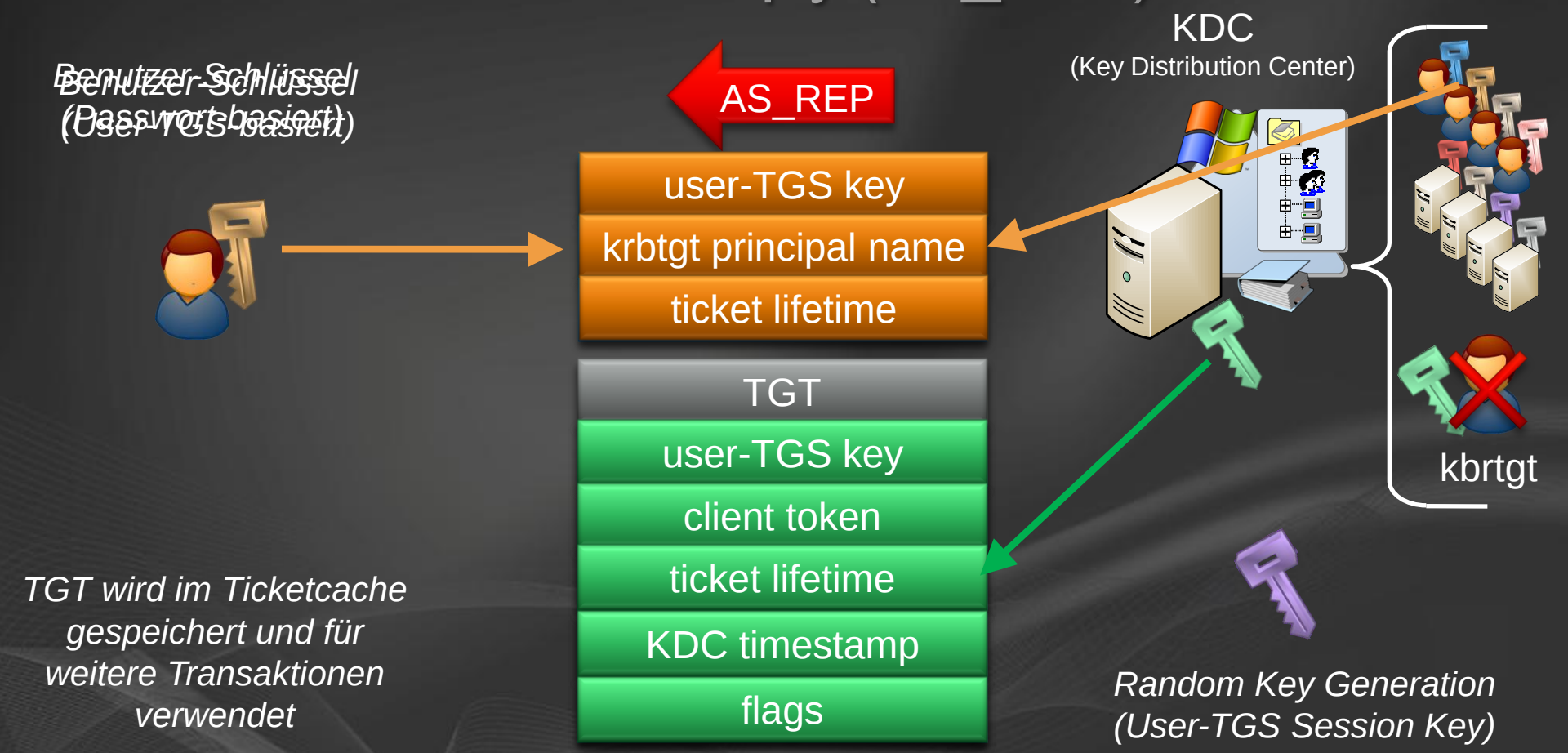
- Verschlüsselung stellt sicher, dass nur befugte Security Principals die Tickets lesen können
  - Ab Windows 2008 / Vista wird Suite-B verwendet!

Funktionsweise von Kerberos
Kerberos Pre-Authentifizierung



- Der KDC kann eine Pre-Authentifizierung verlangen, um Brute-Force und Dictionary-Angriffe zu erschweren
  - Timestamp wird mit dem Benutzerschlüssel ver/entschlüsselt
  - Timestamps müssen innerhalb der Toleranzgrenze (5 Min) liegen
  - Pre-Authentifizierung ab W2000 Security Principals aktiviert

Funktionsweise von Kerberos
Authentication Server Reply (AS_REP)



- Das TGT hat eine Haltbarkeit von 10 Stunden (default)
- Ein Renewal ist innerhalb von 7 Tagen möglich (default)

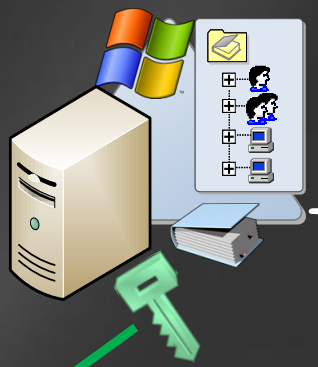
Funktionsweise von Kerberos
Service Ticket Request (TGS_REQ)

Benutzer-Schlüssel
(User-TGS-basiert)

TGS_REQ

service principal
requestes lifetime
TGT
user-TGS key
client token
ticket lifetime
KDC timestamp
flags
Authenticator
client timestamp

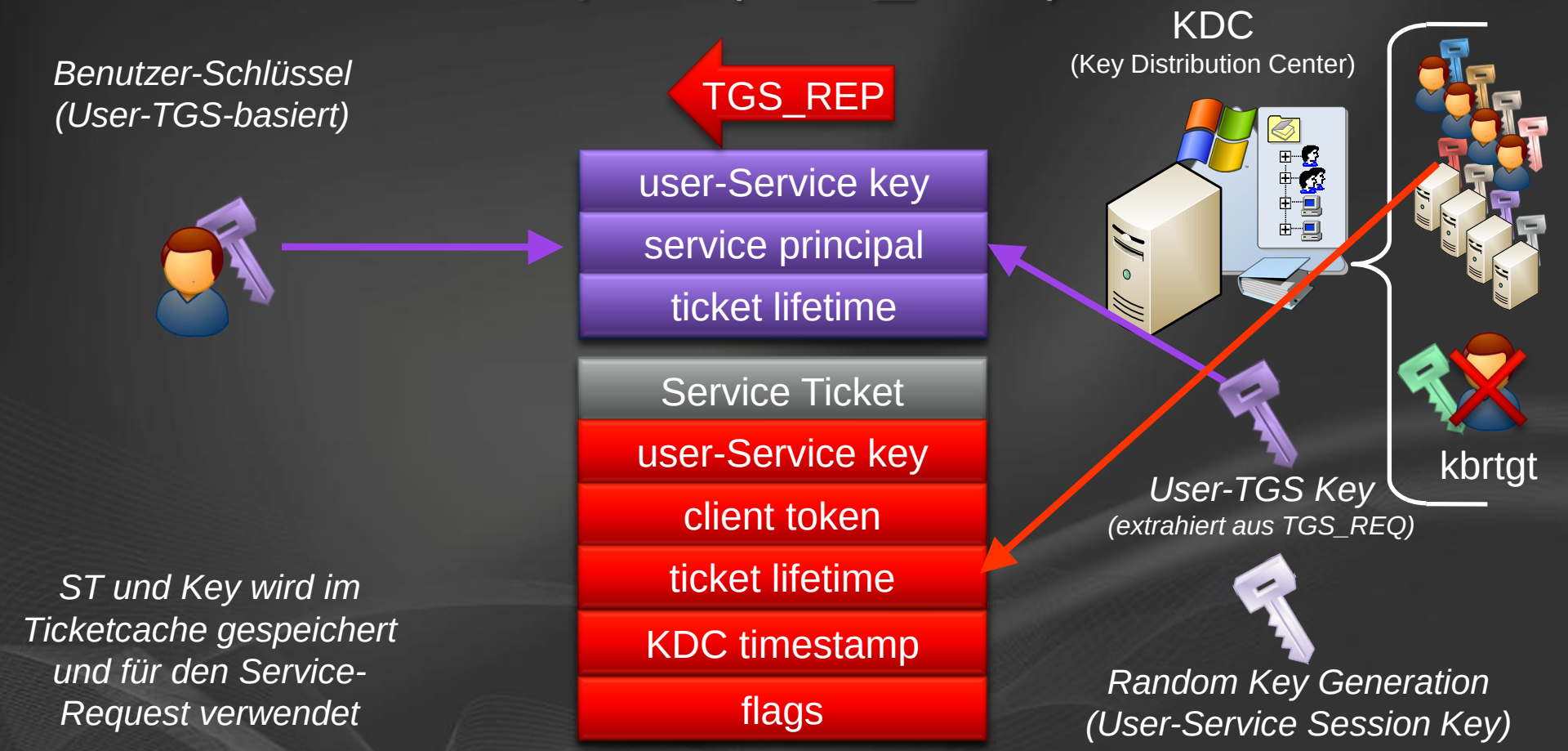
KDC
(Key Distribution Center)



kbrtgt

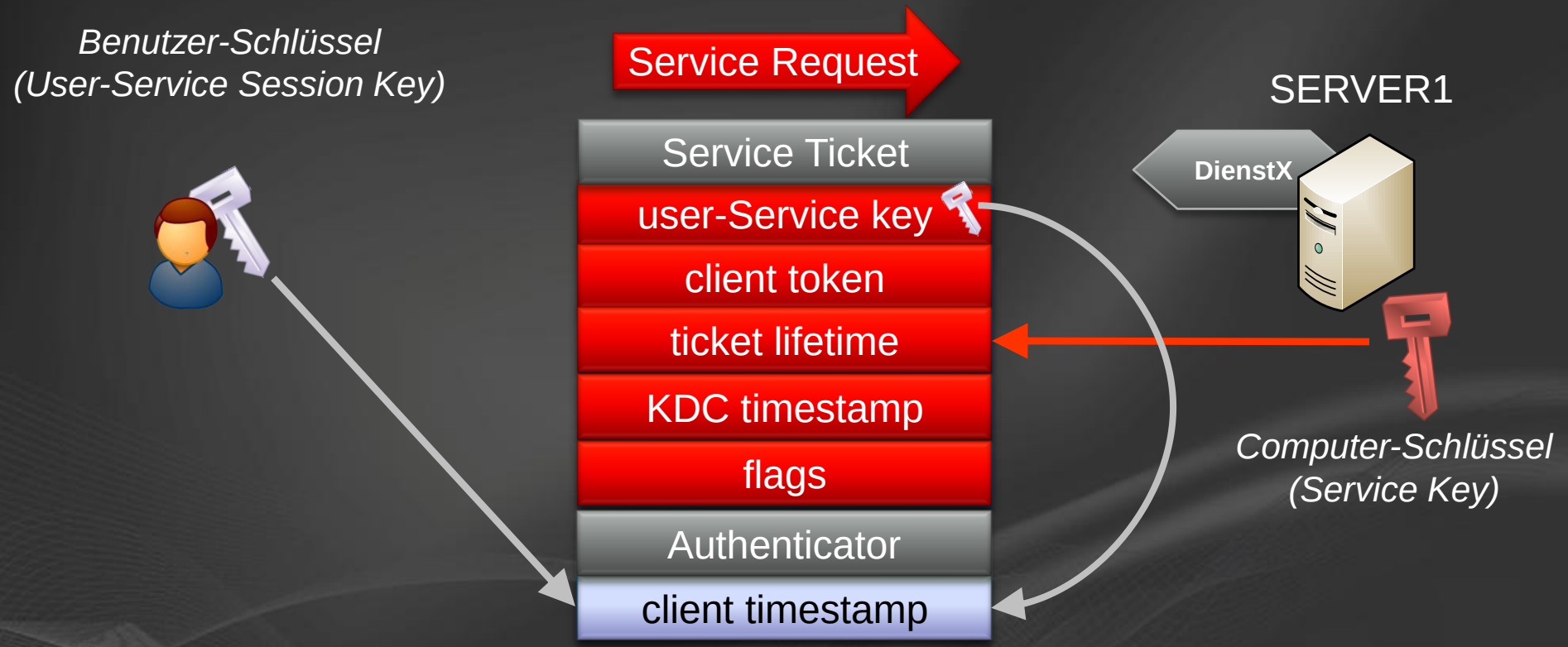
- KDC extrahiert den User-TGS Key aus dem TGT
- Uhrzeit im Authenticator dient zur Re-Authentifizierung

Funktionsweise von Kerberos
Service Ticket Request (TGS_REP)



- Das ST hat eine Haltbarkeit von 600 Minuten (default)

Funktionsweise von Kerberos
Zugriff auf den Service



- Uhrzeit im Authenticator dient erneut der Authentifizierung
- User-Service Sessions Keys bieten Secure-Channels
  - z.B. IPSec und SSL-Verbindungen ohne Zertifikate

Agenda

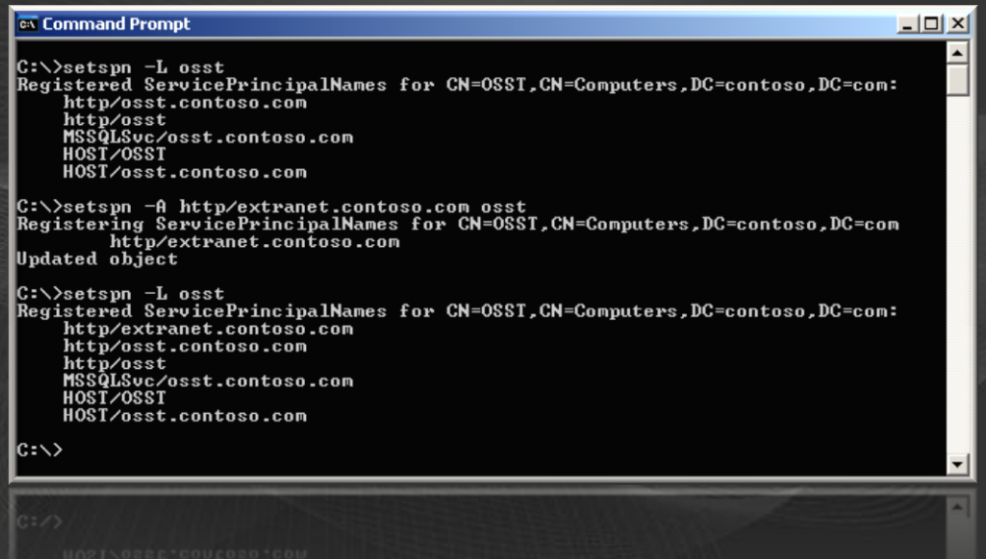
- 1x1 der Authentifizierung und Authorisierung
  - Trusted Subsystem vs. Impersonation Model
  - Prozesskonten und Zugriffe auf Ressourcen
- Deep Dive in das Kerberos Protokoll
  - Authentifizierung und Zugriffe auf Ressourcen
  - Kerberos Service Principal Names (SPNs)
  - Kerberos Delegation und W2K3 Extensions
    - Kerberos Constrained Delegation (A2D2)
    - Kerberos Protocol Transition (T2A4D)
- Zusammenfassung und Ressourcen

Service Principal Names (SPNs)
Allgemeines

- Bei der Service-Ticket-Anfrage wird der Service Principal Name (SPN) übergeben
  - Die Client Anwendung legt den verwendeten SPN fest
  - Der SPN wird vom KDC zur Lokalisierung des Active Directory-Kontos benötigt
    - Die SPNs werden im servicePrincipalName Attribut gespeichert
    - SPNs müssen in der Kerberos Realm eindeutig sein
- Jedes Computerkonto hat bereits mehrere SPNs
  - HOST/computername.domain.de
  - Zusätzlich haben sie über 50 vordefinierte SPNs, die nicht im „servicePrincipalName“ Attribut aufgeführt sind
    - http/computername.domain.de
    - cifs/computername.domain.de
    - ...

Service Principal Names (SPNs)
Eigene SPNs registrieren

- Um sich an einem Dienst zu authentifizieren, muss der verwendete SPN dem Security Principal zugeordnet sein, der den Dienst ausführt.
  - Bei Network Service, Local Service oder Local System
    - SPNs werden dem jeweiligen Computerkonto zugeordnet
  - Werden Active Directory-Benutzerkonten verwendet
    - SPNs werden dem jeweiligen Benutzerkonto zugeordnet



„SETSPN.EXE“ ist im Windows Server 2008 nun enthalten und unterstützt neue CMD Switches.
-R = Resetet den HOST SPN
-Q = Nach SPNs suchen.
-X = Duplicate Check für SPNs
-S = Add mit Duplicate Check

Service Principal Names (SPNs)
Bekannte Stolperfallen!

- Internet Explorer fordet nicht eindeutige SPNs an
  - Verwendete URL in der Adressbar: http://srv:8000/
  - Angefordert wird „http/srv“ anstelle von „http/srv:8000“
- Wenn Benutzerkonten verwenden werden, sollte nicht der Rechnername als SPN genutzt werden
  - Built-In SPNs existieren bereits und können kollidieren
  - Ports werden von den Anwendungen oft ignoriert
  - DNS-Aliase und HTTP Hostheader sind die Lösung!
- IIS7 Feature: Kernel-Mode Authentication
  - HTTP.SYS übernimmt die Kerberos Authentifizierung
    - SPNs werden hierbei dem Computer Konto zugewiesen
    - Bei Bedarf über die IIS MMC oder CMD deaktivierbar

{ Kerberos Konfiguration }

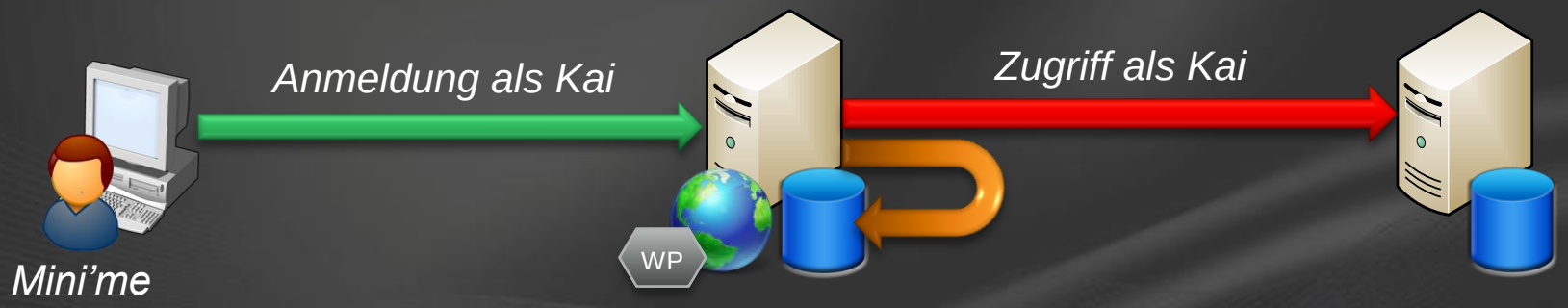
Kai Wilke
Consultant IT-Security
MVP ISA Server und Security (a.D.)
mailto:kw@itacs.de

Agenda

- 1x1 der Authentifizierung und Authorisierung
  - Trusted Subsystem vs. Impersonation Model
  - Prozesskonten und Zugriffe auf Ressourcen
- Deep Dive in das Kerberos Protokoll
  - Authentifizierung und Zugriffe auf Ressourcen
  - Kerberos Service Principal Names (SPNs)
  - Kerberos Delegation und W2K3 Extensions
    - Kerberos Constrained Delegation (A2D2)
    - Kerberos Protocol Transition (T2A4D)
- Zusammenfassung und Empfehlungen

Kerberos Delagation und Extensions
Nutzen von Kerberos Delegation

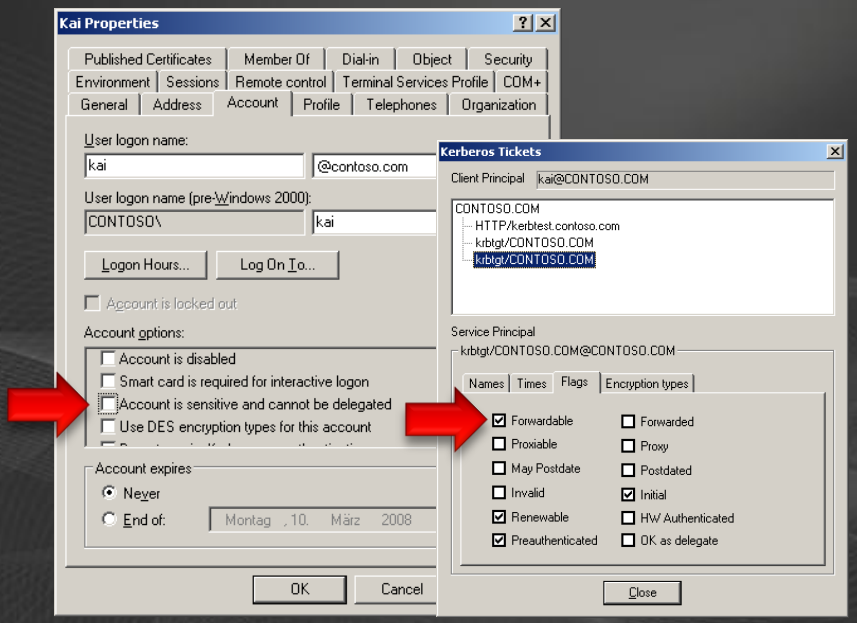
- Delegation ermöglicht einer Anwendung, Kerberos-Tickets an Back-End-Dienste weiterzuleiten.
- Active Directory steuert, welche Security Principals Kerberos im welchem Umfang delegieren können.



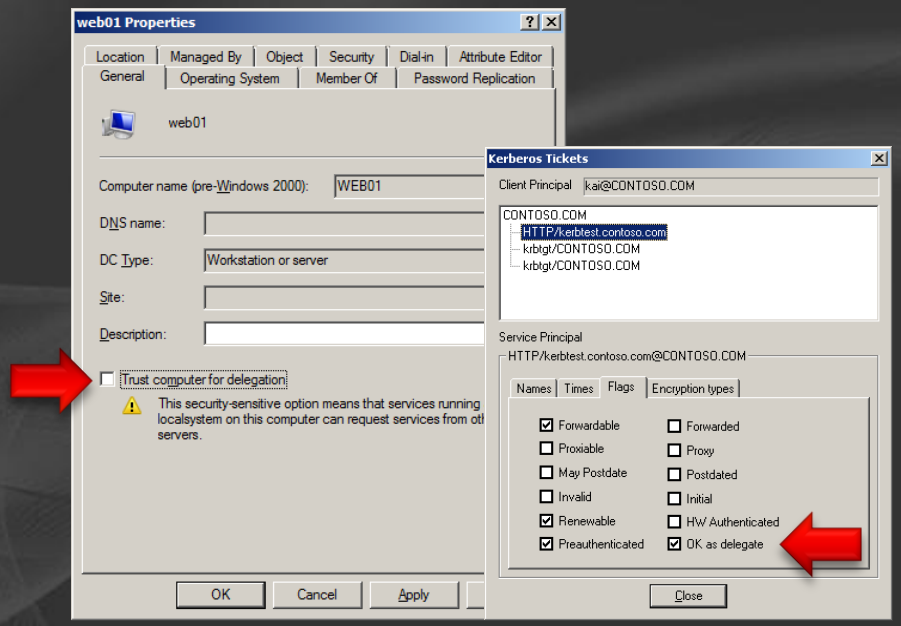
Anwendungsidentität	Lokaler Zugriff	Remote Zugriff
Network Service	Kai	Kai
Local Service	Kai	Kai
Local System	Kai	Kai
Dom Account: WEB1	Kai	Kai

Kerberos Delagation und Extensions
Kerberos Delegation flags

- Active Directory Attribute steuern Kerberos Flags
  - Benutzer-Konto: Darf der Benutzer delegiert werden?
  - Service-Konto: Darf der Service Kerberos delegieren?
- Beide Bedingungen müssen erfüllt sein

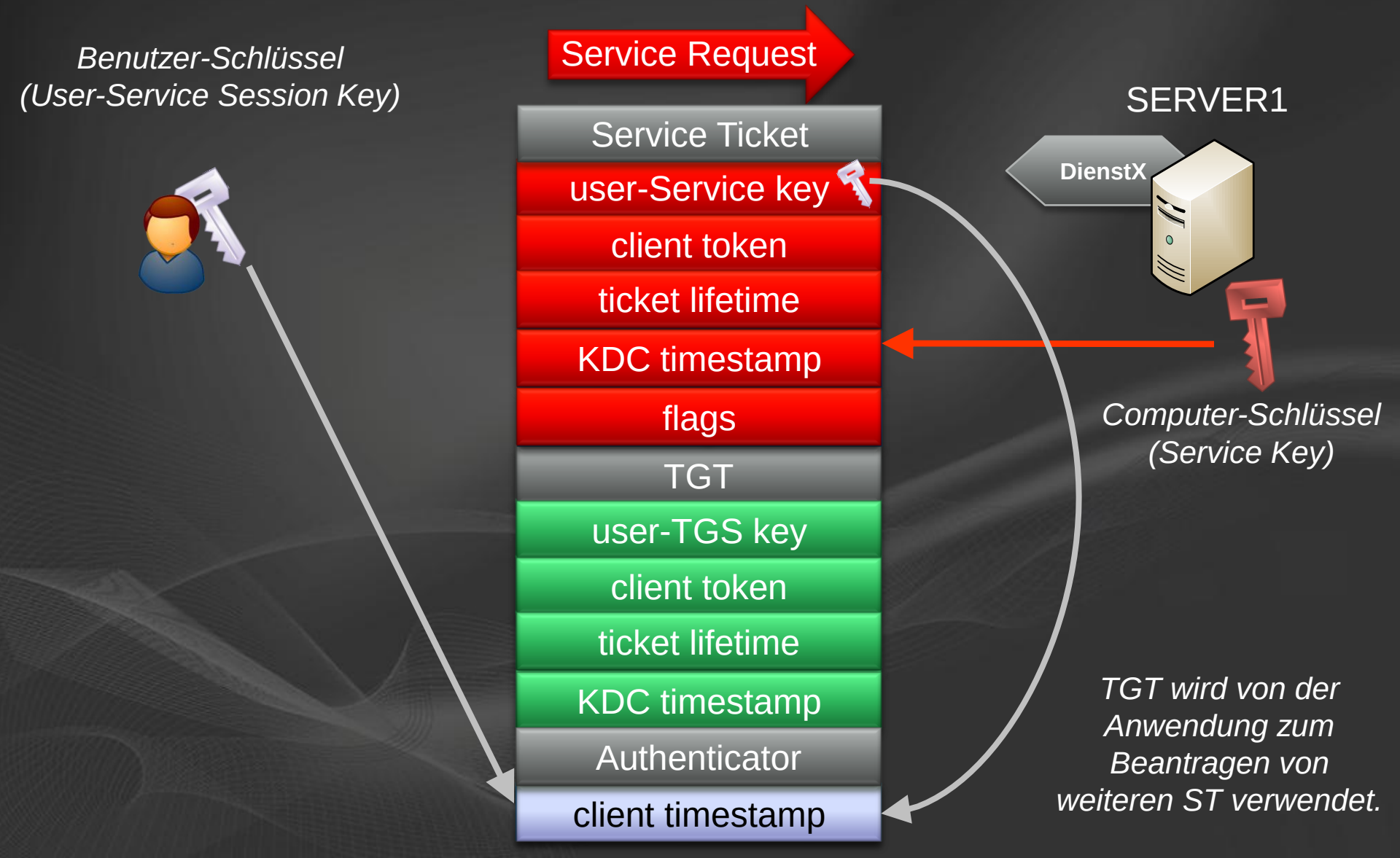


Benutzer TGT ist „Forwardable"

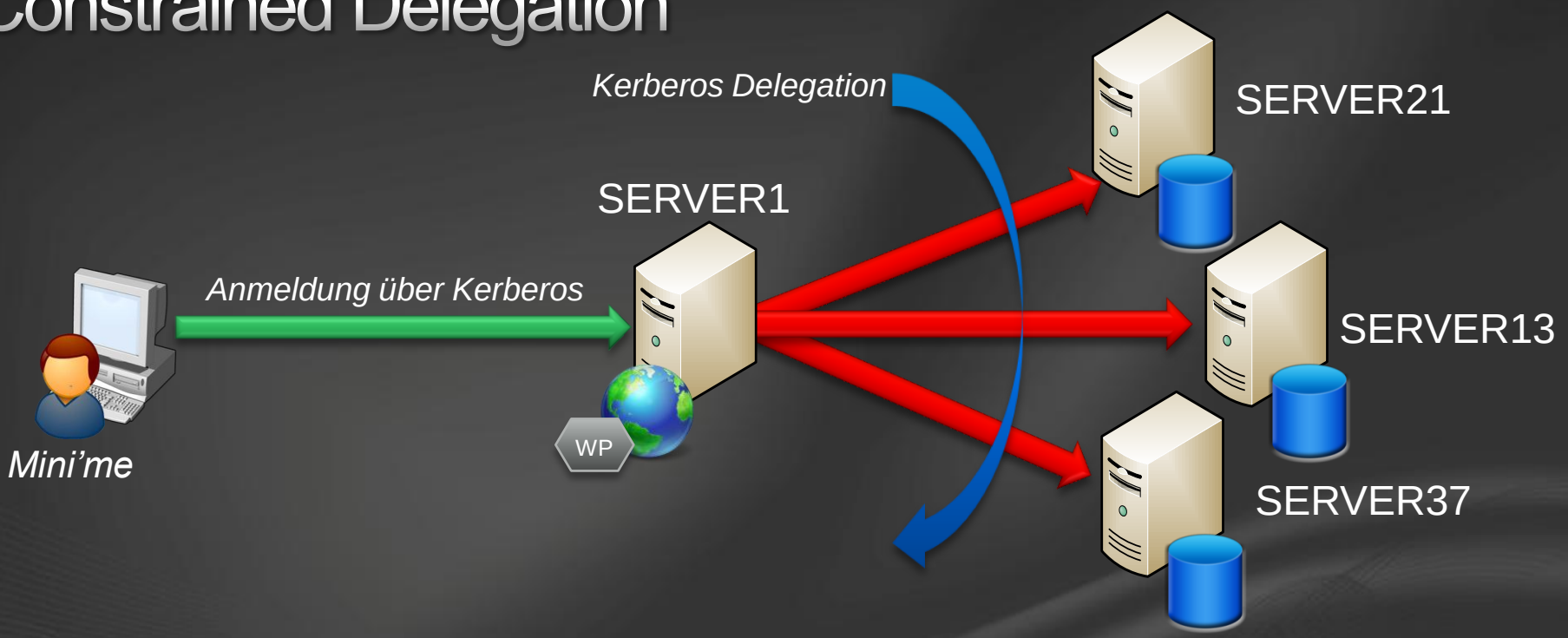


Service Account ist „OK as delegate"

Funktionsweise von Kerberos
Zugriff auf den Service

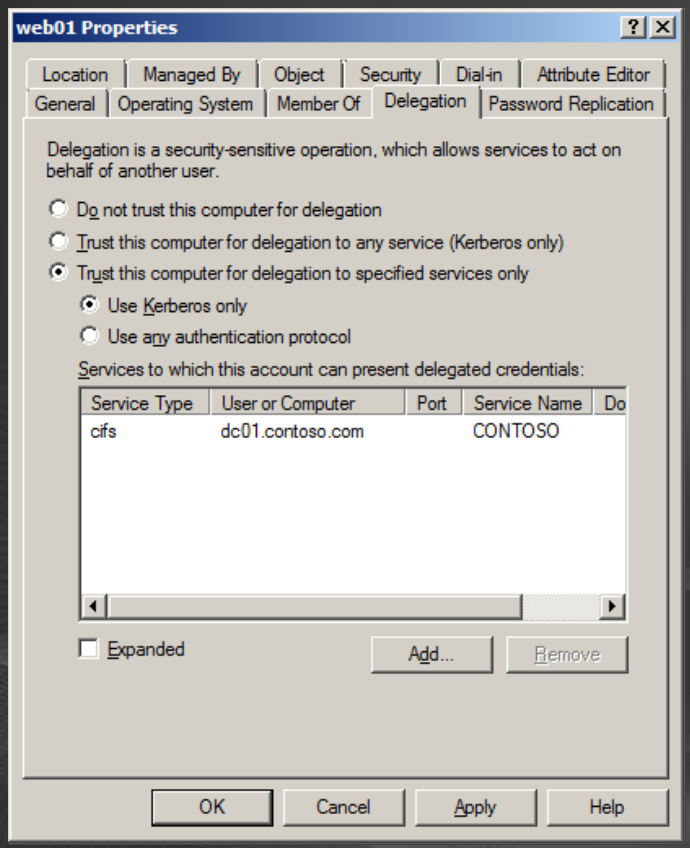


Funktionsweise von Kerberos
Constrained Delegation



- Nachdem die Kerberos Delegation aktiviert wurde, kann das Service-Konto unter Verwendung von Kai‘s Identität auf das gesamte Netzwerk zugreifen.
- Windows 2003 ermöglicht die Einschränkung der Kerberos Delegation (constraining), in dem vom KDC gefiltert wird, zu welchen Zielen die Delegierung geschehen kann.

Funktionsweise von Kerberos
Constrained Delegation (A2D2 Extension)



- Constrained Delegation wird nur im Windows 2003/8-Modus unterstützt
  - „Use Kerberos only“
    - Unterstützt nur Kerberos-Anmeldungen
  - „Use any authentication protocol“
    - Ermöglicht „Protocol Transition“
- Die SPNs legen fest, welche Tickets vom Konto angefragt werden können
  - msDS-AllowedToDelegateTo Attribut

Funktionsweise von Kerberos
Protocol Transition (T2A4D Extension)

- Kerberos kommt fast nur im Intranet zum Einsatz
  - Internet und Extranets haben kein Zugriff auf die KDCs
  - Nicht jede Anwendung unterstützt Kerberos
    - Basic (Sonderfall: IIS reauthentifiziert via Kerberos)
    - WDigest
    - NTLM
    - Forms
    - Zertifikate
    - One Time Password (OTP)
- T2A4D Extension erlaubt es einem Dienstkonto, Kerberos Tickets vom KDC ohne Benutzerinteraktion anzufragen
  - Anwendung steuert, wie/wann/ob ein Benutzer authentifiziert wird
    - Active Directory Credentials werden hierbei nicht benötigt
    - Anwendung sollte demnach sehr vertrauenswürdig sein!
  - Restriktionen über „Sensitiv“-Flag und „A2D2”-Einstellungen

Funktionsweise von Kerberos
Konfiguration der Protocol Transition

- Zugriff über .NET/WindowsIdentity oder W32/LsaLogonUser
- Lokale Zugriffe: Services For User to Self (S4U2S)
  - Ermöglicht einem Dienst ein Benutzer Token zu erzeugen
  - Anwendung braucht „Act as Part of the Operating System“
    - Ohne „SeTCBPrivilege“: Service erhält „Identification Token“
    - Mit „SeTCBPrivilege“: Service erhält „Impersonation Token“
  - Ein Impersonation Token ermöglichen eine lokale Impersonation
    - Systemrecht „SeImpersonationPrivilege“ wird hierfür benötigt
  - Kerberos Konfigurationen ist hierfür nicht notwendig
- Remote Zugriffe: Services for User To Proxy (S4UTP)
  - Ermöglicht den Dienst eine Kerberos Delegation zu nutzen
    - Aktivieren der Contrained Delegation am Quell-Dienst
    - Die Option “Any Protocol” muss hierbei ausgewählt werden
    - SPNs auswählen die vom Dienst angefragt werden können
  - Je nach Anwendung ist eine lokale Impersonation notwendig

{ Kerberos Delegation }

Kai Wilke
Consultant IT-Security
MVP ISA Server und Security (a.D.)
mailto:kw@itacs.de

Agenda

- 1x1 der Authentifizierung und Authorisierung
  - Trusted Subsystem vs. Impersonation Model
  - Prozesskonten und Zugriffe auf Ressourcen
- Deep Dive in das Kerberos Protokoll
  - Authentifizierung und Zugriffe auf Ressourcen
  - Kerberos Service Principal Names (SPNs)
  - Kerberos Delegation und W2K3 Extensions
    - Kerberos Constrained Delegation (A2D2)
    - Kerberos Protocol Transition (T2A4D)
- Zusammenfassung und Ressourcen

Zusammenfassung

- Sichere Kerberos Constrained Delegation und Protocol Transition benötigt etwas Know-How
  - Reden Sie mit den Entwicklern/Administratoren und bewerten sie den Nutzen und etwaige Sicherheitsrisiken
- Wenn eine Kerberos Delegation benötigt wird, verwenden Sie unbedingt Constrained Delegation
  - Nutzen Sie die „T2A4D“ Erweiterung mit Vorsicht!
  - Markieren Sie ihre priviligierte Konten als „sensitiv“!
- Verwenden Sie am besten dedizierte Dienstkonten
  - Computerkonten werden von vielen Diensten verwendet
  - SPNs werden werden nur bei der ST-Anfrage validiert
- Konfigurieren Sie die verwendeten SPNs gründlich

Windows Server 2008
weitere Ressourcen

- Windows Server 2008 Tech Center
  http://www.microsoft.com/germany/technet/prodtechnol/windowsserver/2008/default.mspx
- Windows Server 2008 Webcasts:
  http://www.microsoft.com/germany/technet/webcasts/windowsserver2008.mspx
- Windows Server 2008 Produktseite:
  http://www.microsoft.com/germany/windowsserver2008/default.mspx
- Microsoft Virtualization:
  http://www.microsoft.com/virtualization/default.mspx

Ask the Experts

Wir freuen uns auf Ihre Fragen: Technische Experten stehen Ihnen während der gesamten Veranstaltung in der Haupthalle zur Verfügung.

MVP Microsoft Most Valuable Professional

clip Microsoft Community Leader/Insider Program

Microsoft®

Ihr Potenzial. Unser Antrieb.