Defanging the Dog: Attacking Windows Kerberos

Matthew Navarro

General Outline

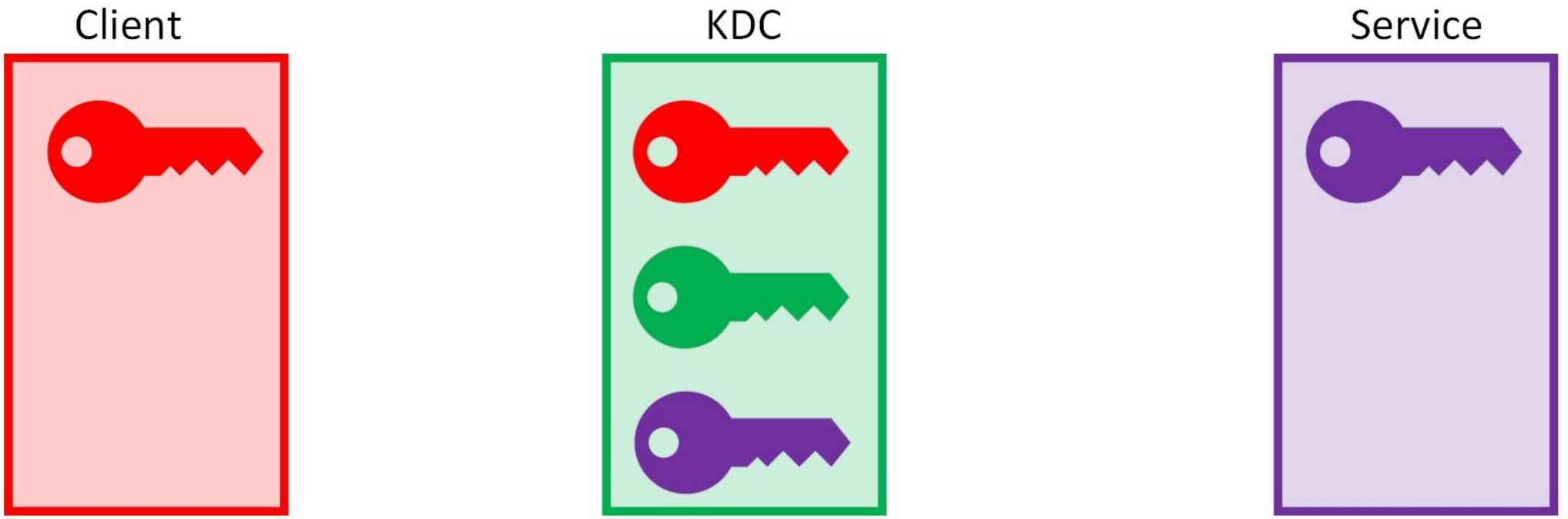
- Review the Kerberos authentication process.
- Overview of the Kerberos landscape
- Analyze some Kerberos attacks
- Create detections with PowerShell

Kerberos Authentication Process

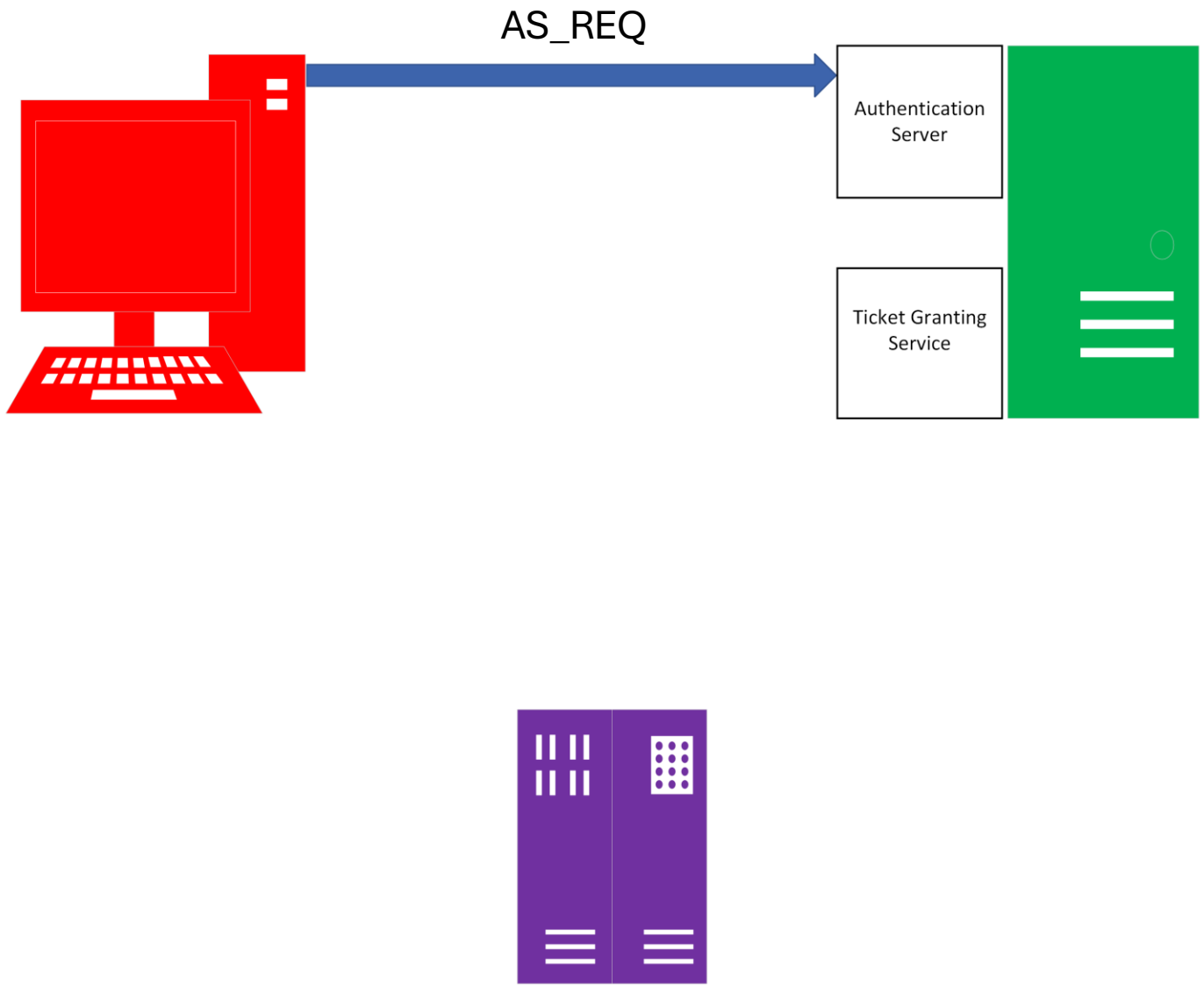
3 Big Key Exchanges

- Client <===> Authentication Server (AS)
- Client <===> Ticket Granting Server (TGS)
- Client <===> Application Server (AP)

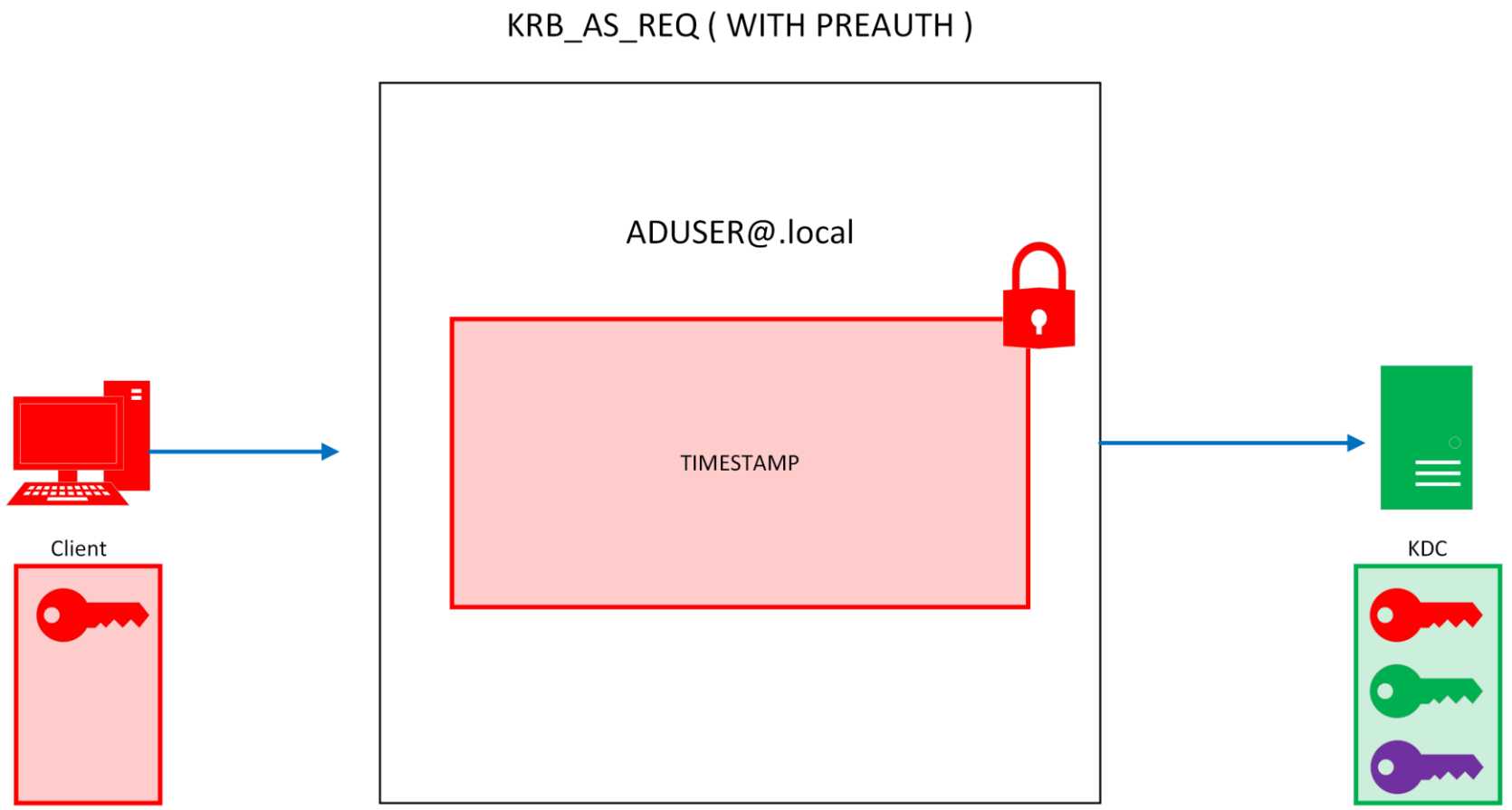
Keys Before Exchanges



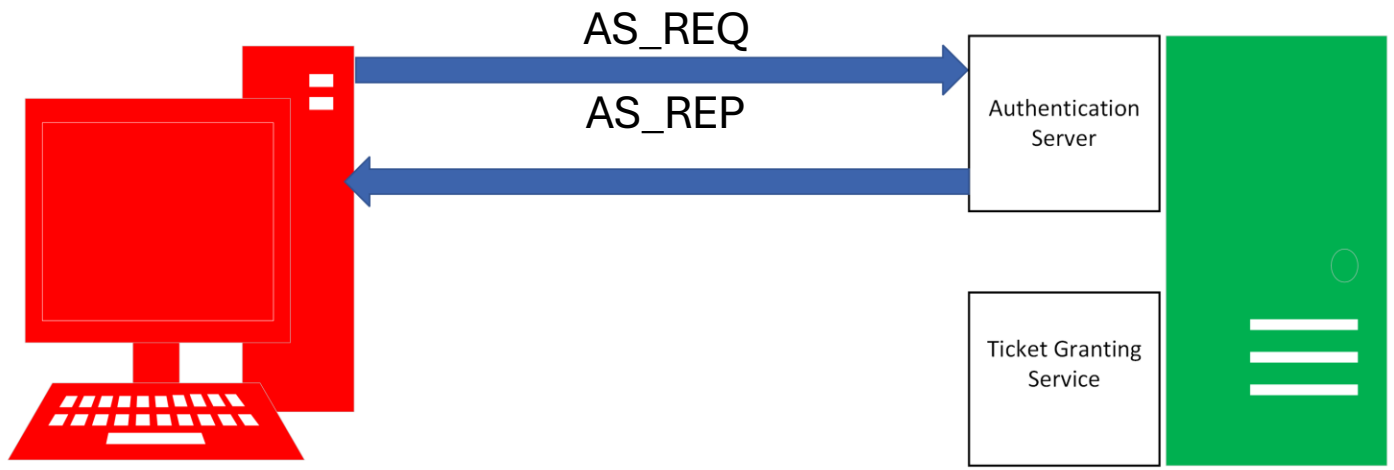
AS Exchange 1

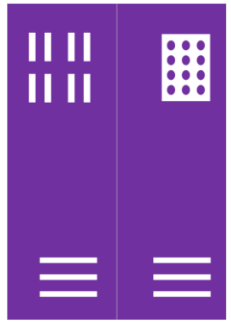


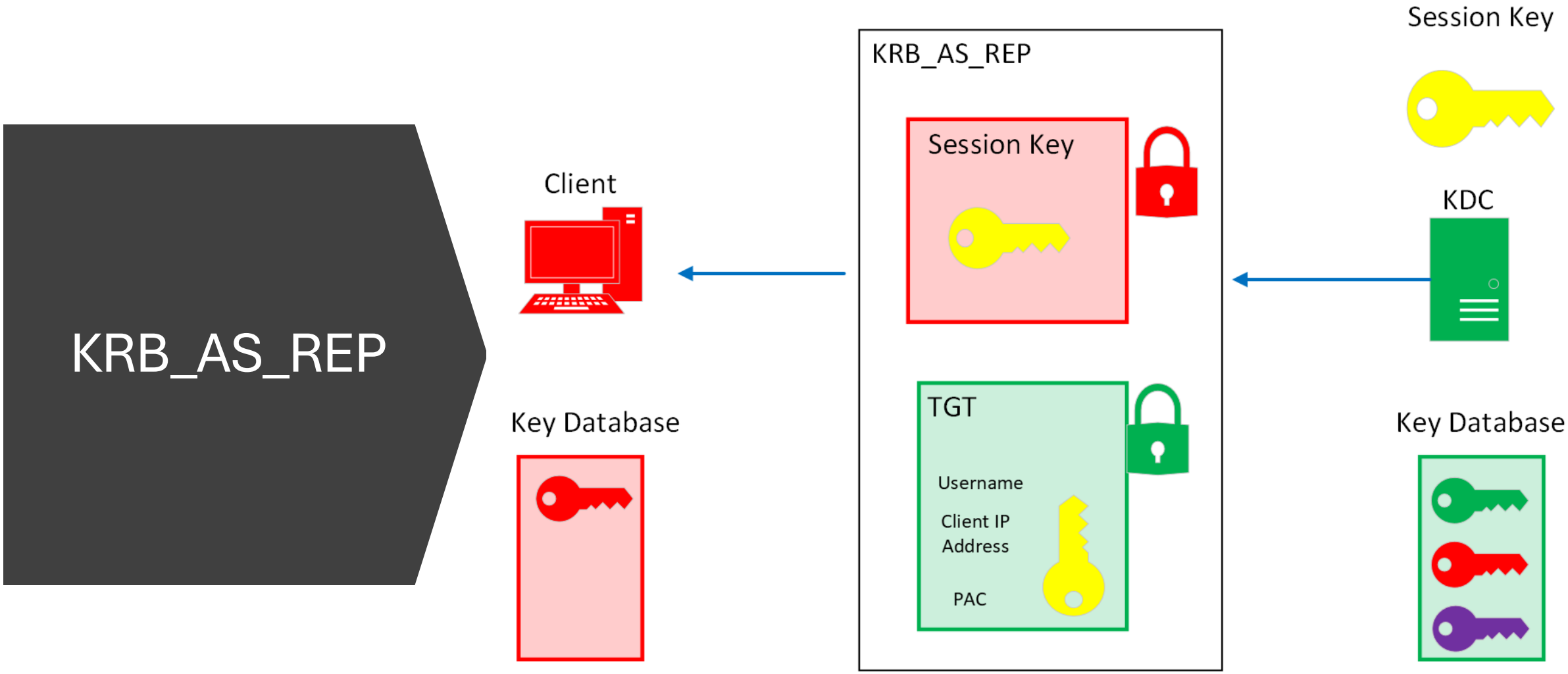
KRB_AS_REQ



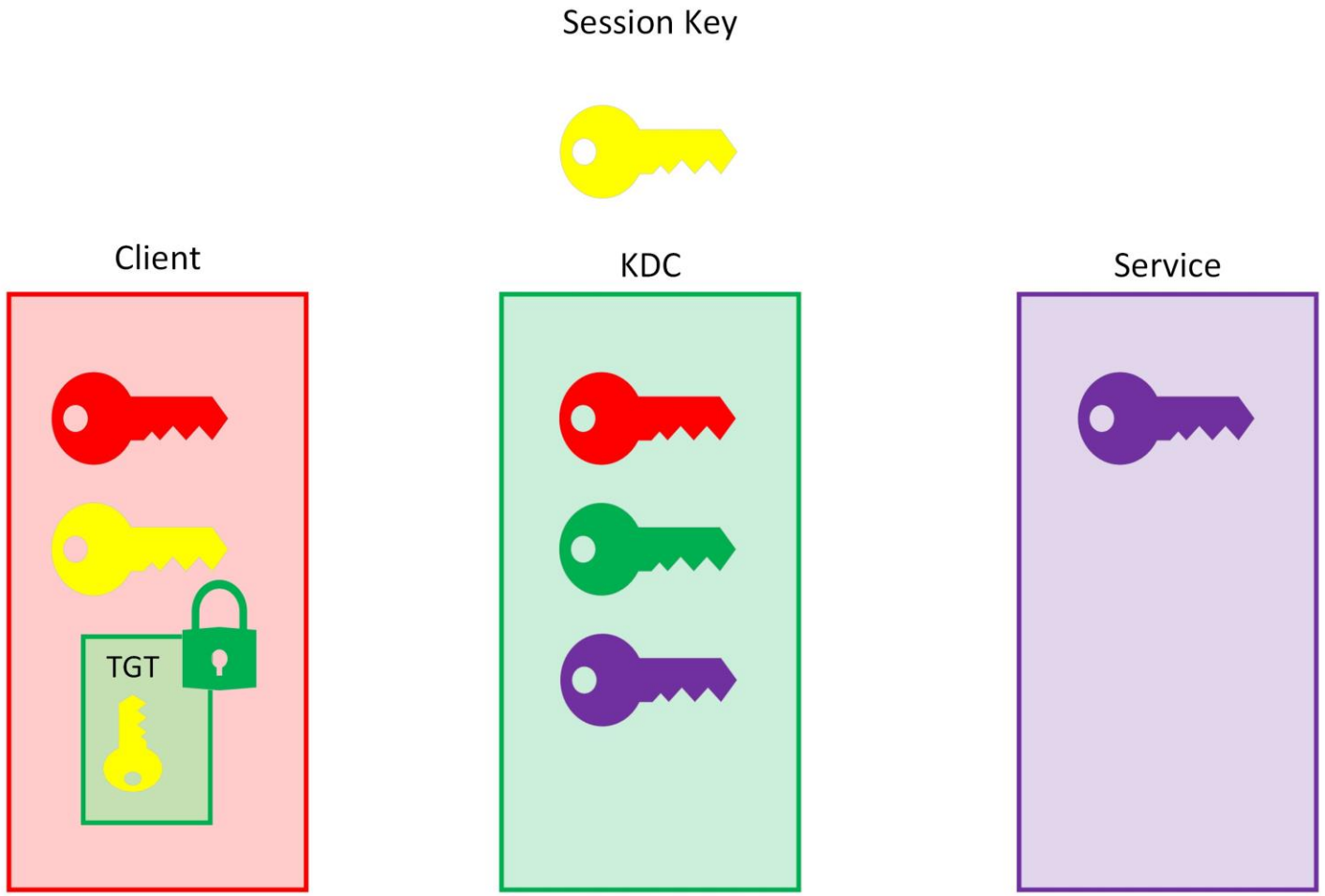
AS Exchange 2





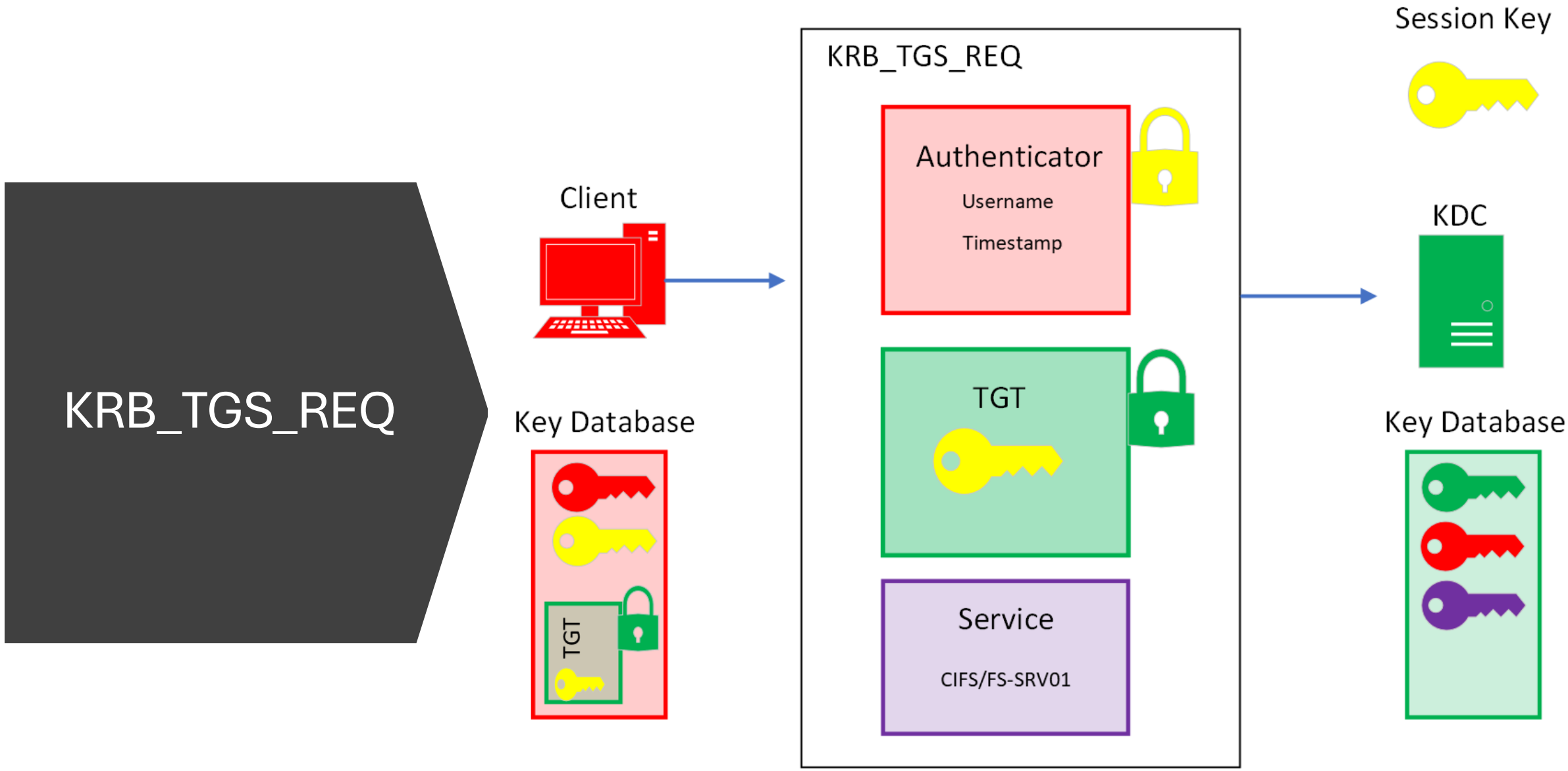

KRB_AS_REP
Client
Key Database
KRB_AS_REP
Session Key
TGT
Username
Client IP Address
PAC
Session Key
KDC
Key Database

Keys After Authentication Service Exchange

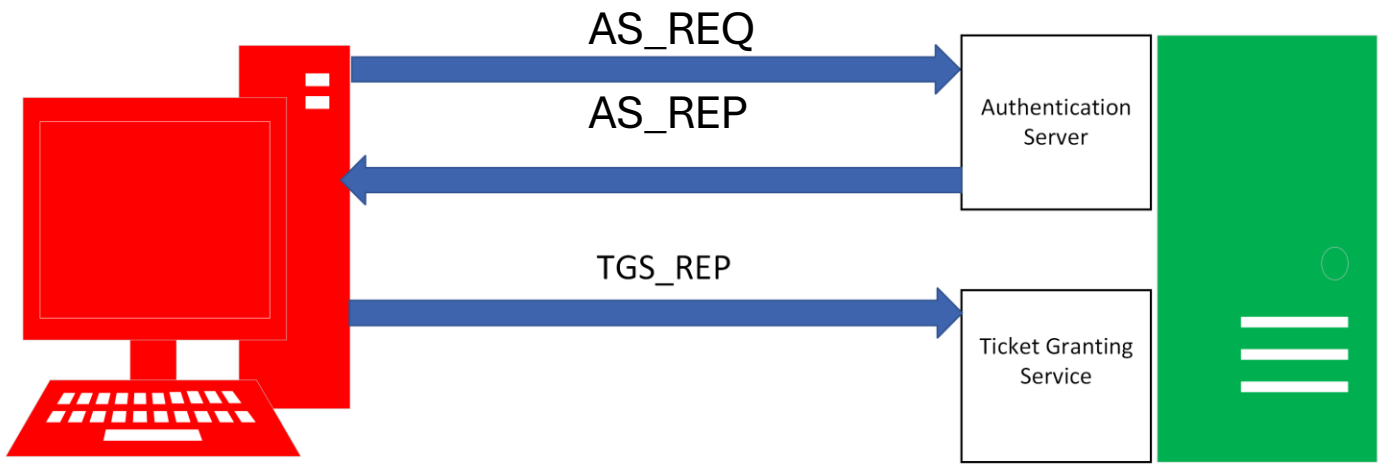


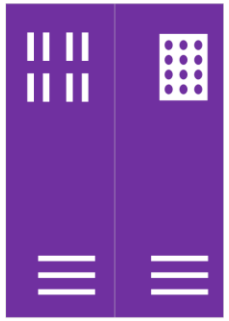
The Authentication Server drops out

- Client has been authenticated as a user in the domain.
- Client can now begin its request for services.
- TGT will be recycled until it expires.


KRB_TGS_REQ
Client
Key Database
TGT
KRB_TGS_REQ
Authenticator
Username
Timestamp
TGT
Service
CIFS/FS-SRV01
Session Key
KDC
Key Database

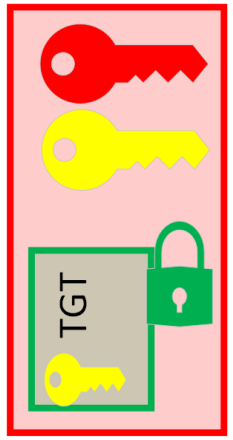
TGS Exchange 1





KRB_TGS_REP

Client



Key Database

KRB_TGS_REP

TGS

CIFS/FS-SRV01

username

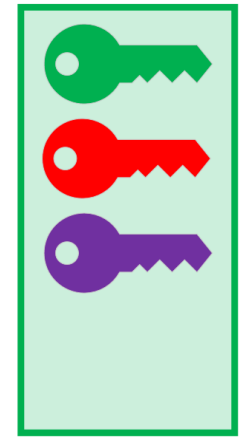
Timestamp

PAC

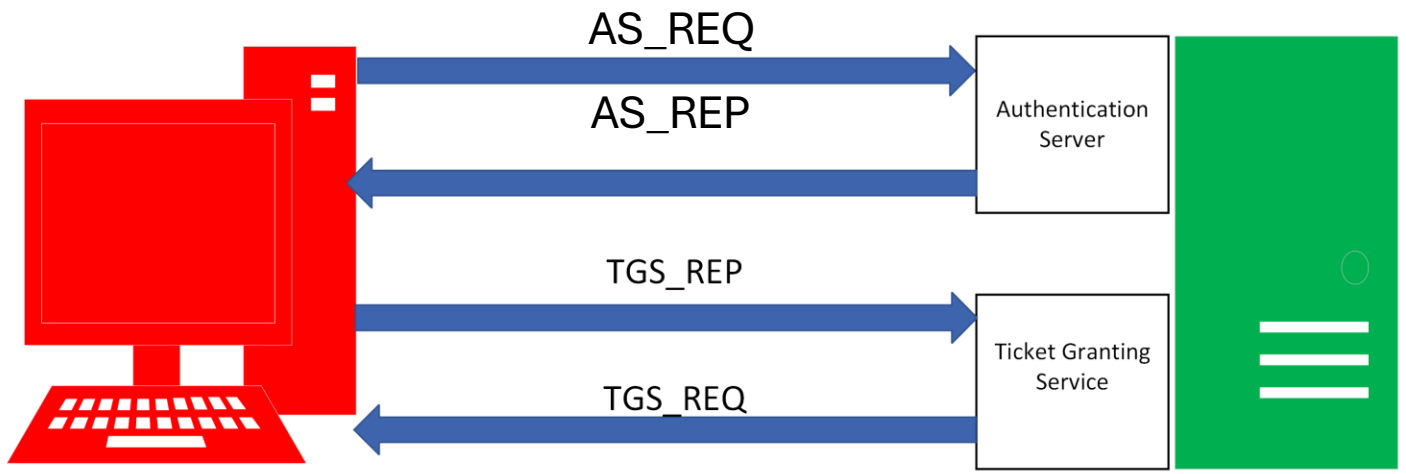
Session Key

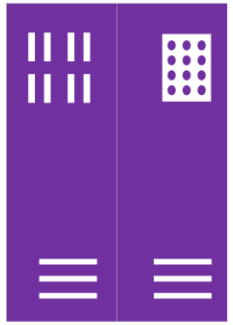
KDC

Key Database

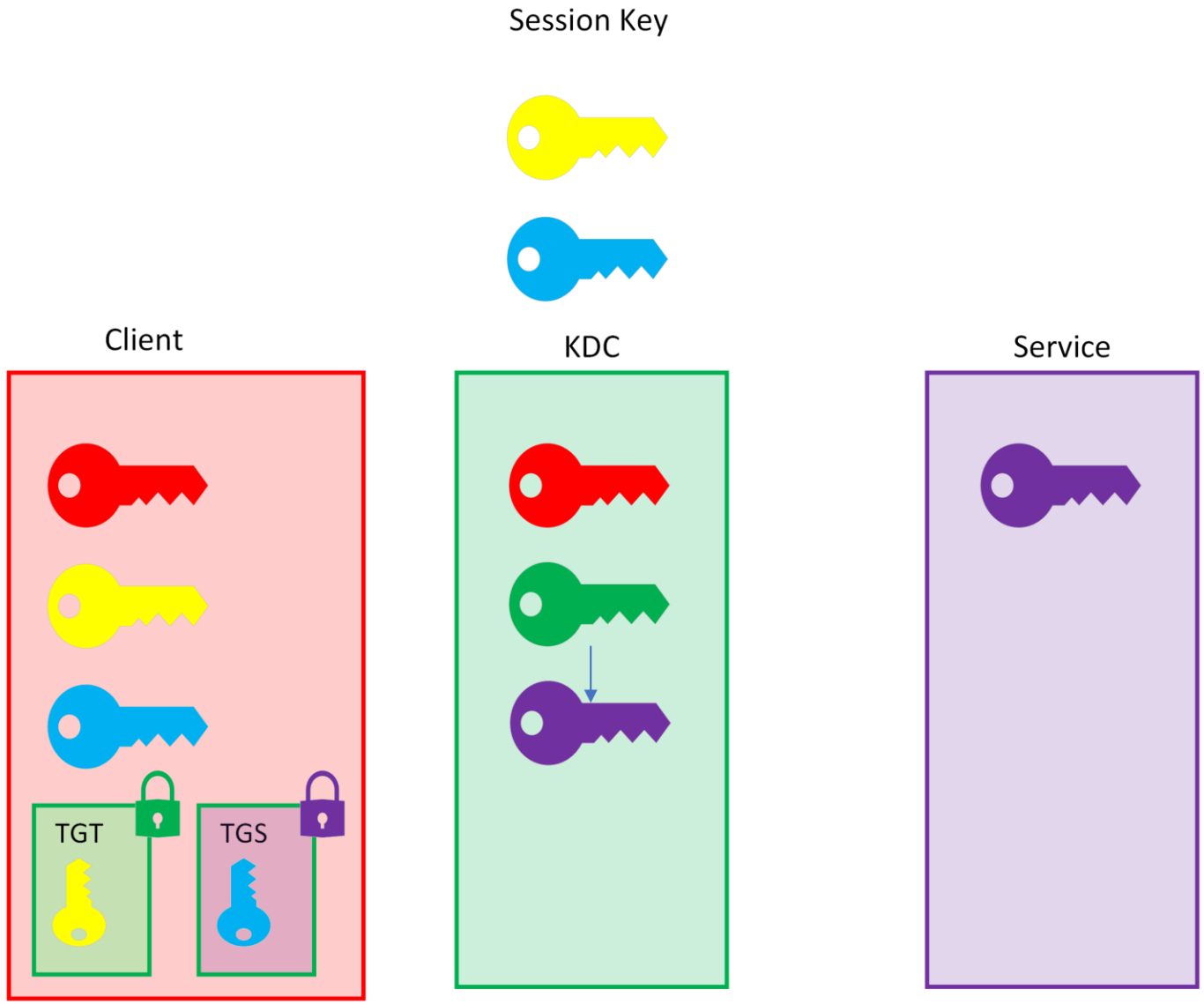


TGS Exchange 2

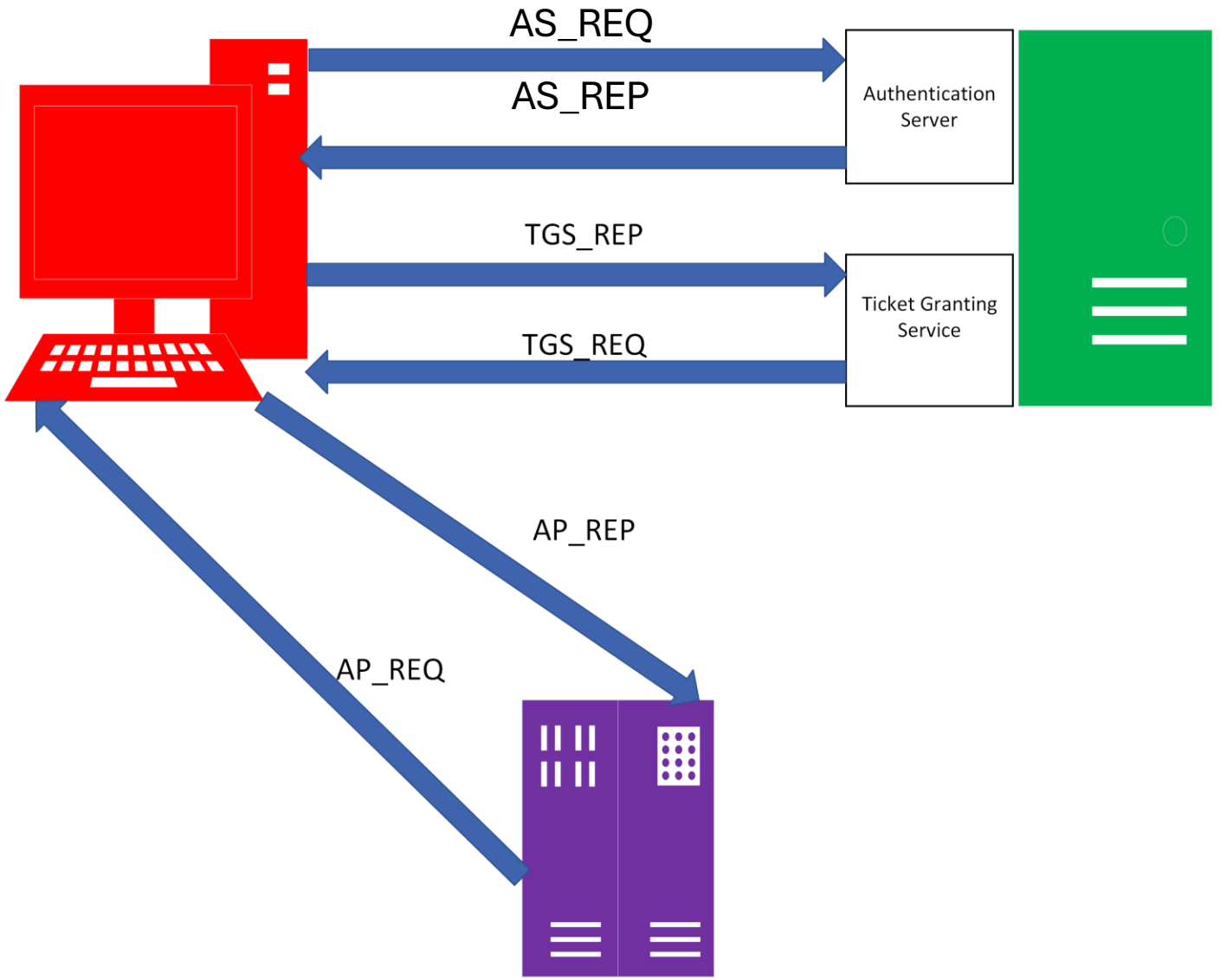




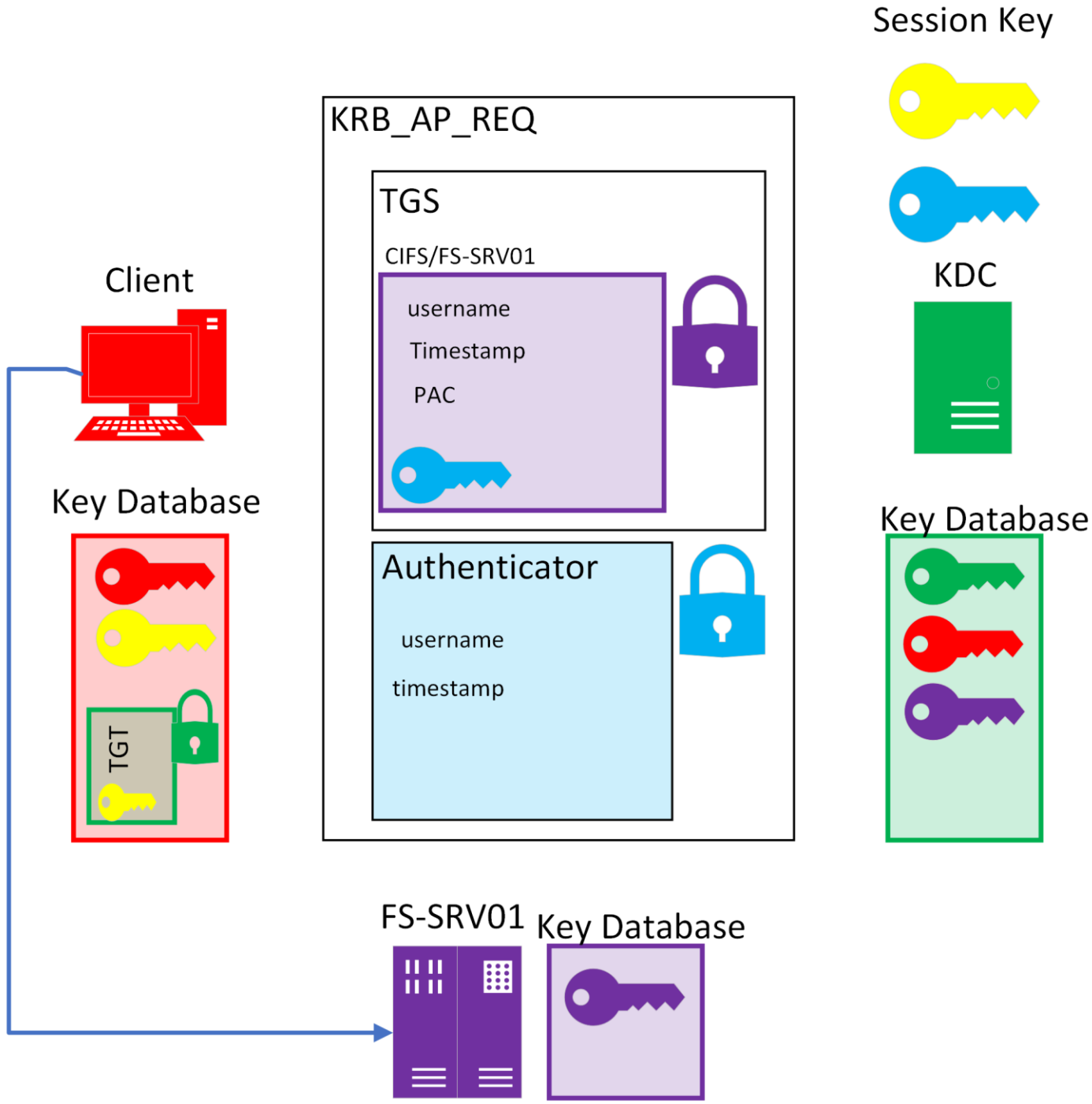
Keys After TGS Exchange



AP Exchange 1



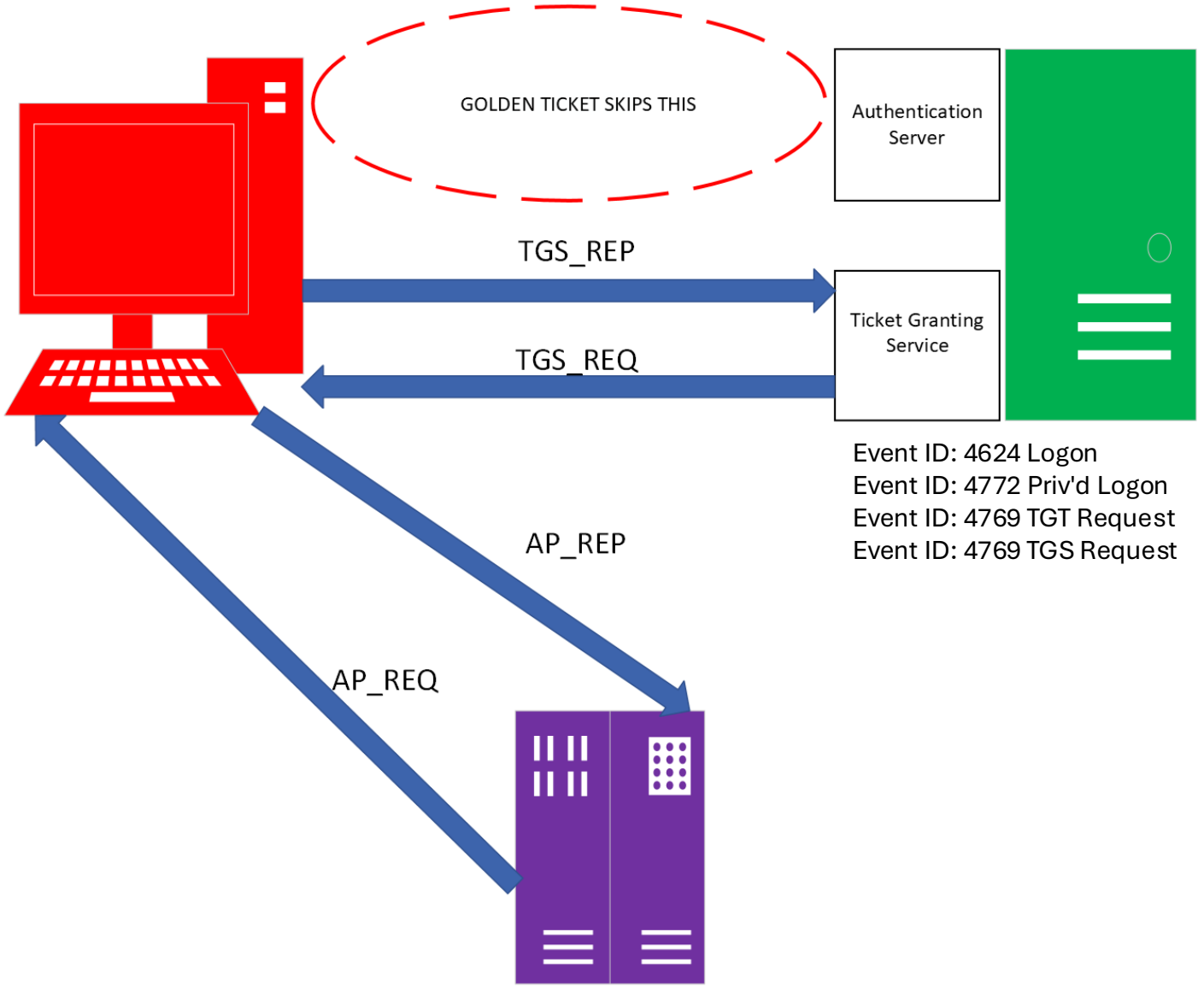
KRB_AP_REQ


Session Key
KDC
Key Database
Client
Key Database
TGT
KRB_AP_REQ
TGS
CIFS/FS-SRV01
username
Timestamp
PAC
Authenticator
username
timestamp
FS-SRV01
Key Database

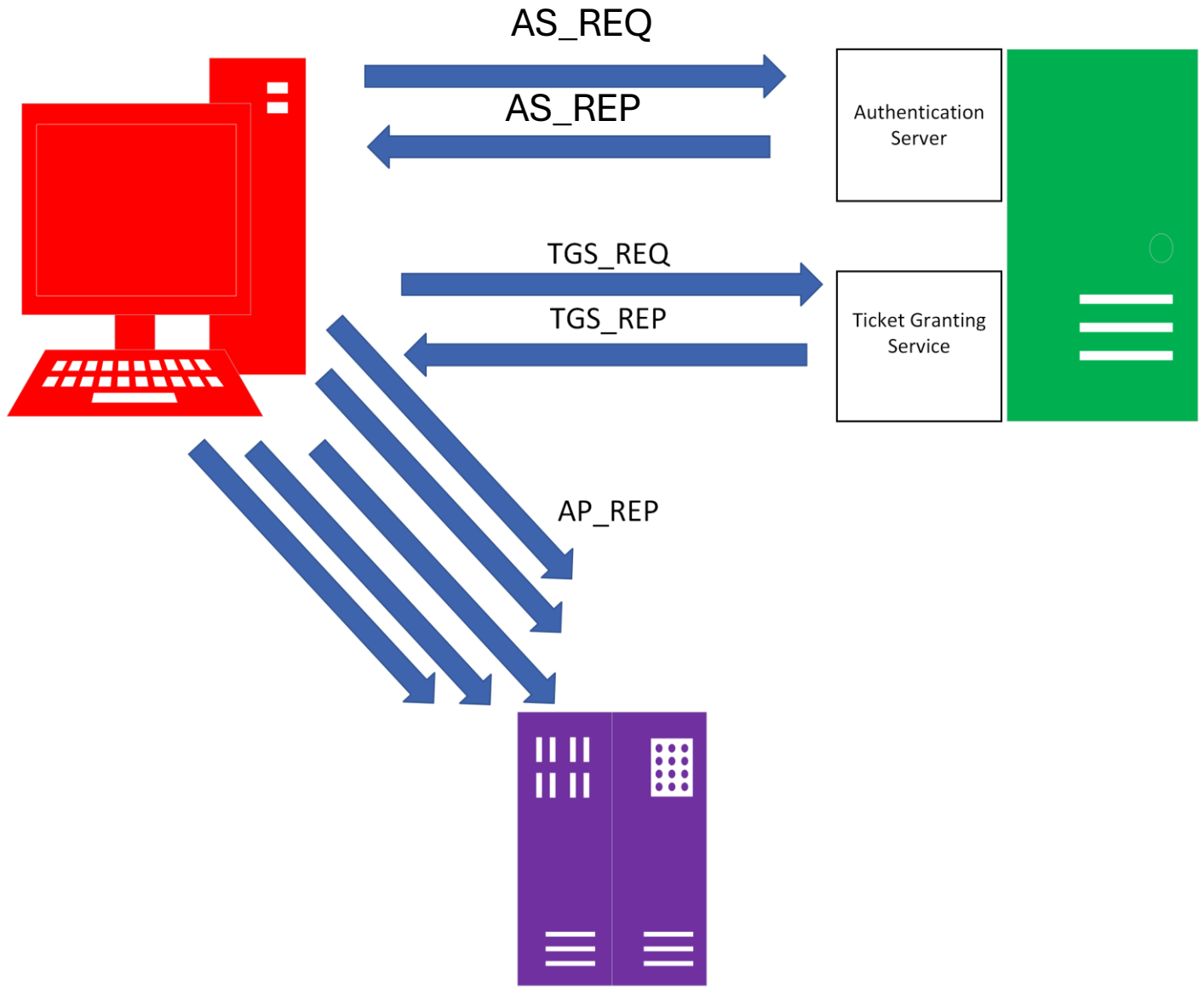
Some famous Kerberos attacks

- AS-REP Roasting (PrivEsc)
- AS-REQ Spamming / Bruteforce (Enumeration/PrivEsc)
- Kerberoasting (PrivEsc) <===
- Golden Ticket (Persistance) <===
- Silver Ticket (Persistance) <===
- Delegation Attacks (PrivEsc)

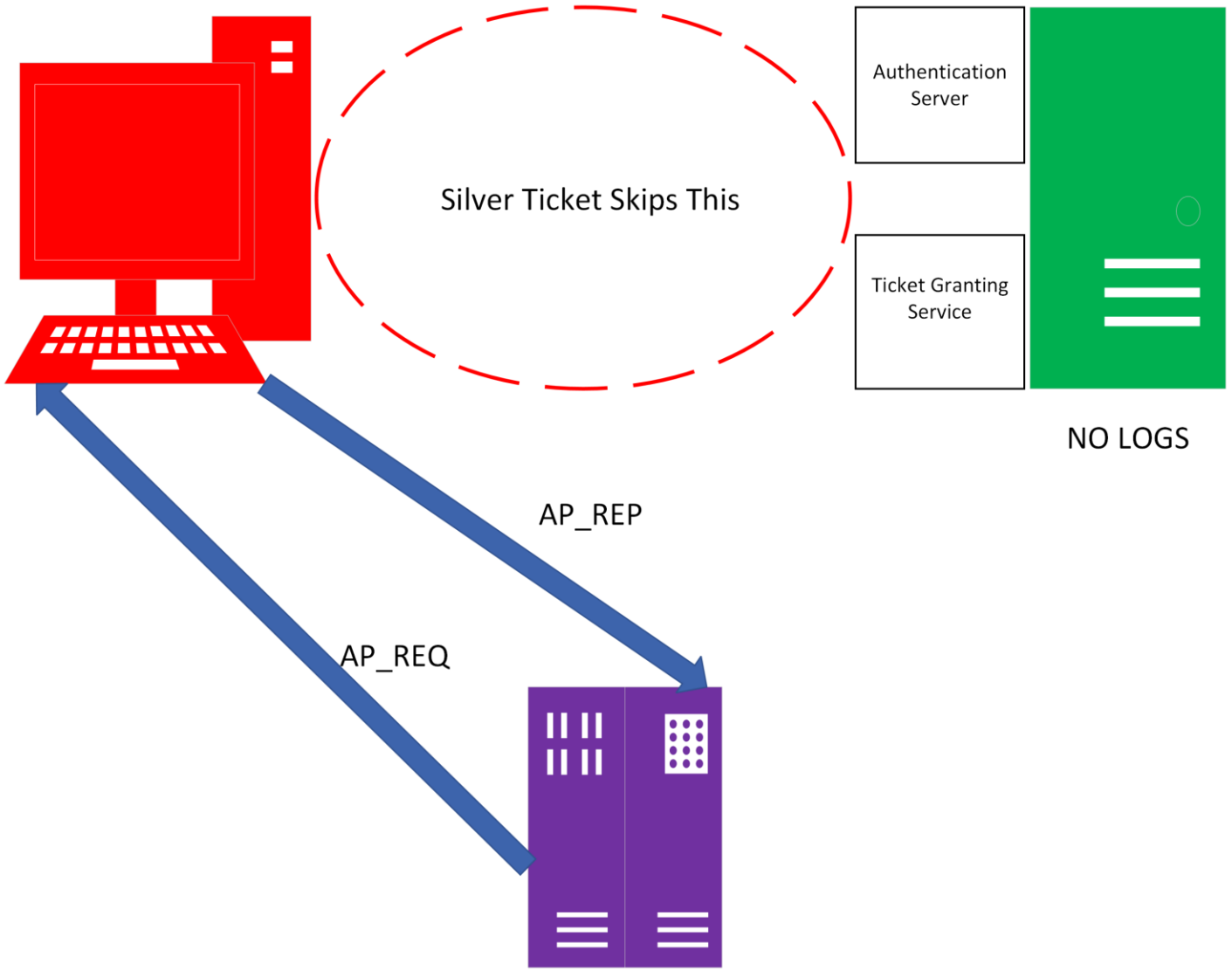
Golden Ticket



Kerberoasting



Silver Ticket



Writing Detections


BREAKING
NEWS


Up time
27:14:25
DATABASE

BrokeBoyz Cyber Kit™

- We may not have the resources to create static IOC's
- Let's make some Behavior detections

BrokeBoyz Cyber Kit™: Catching Golden Tickets

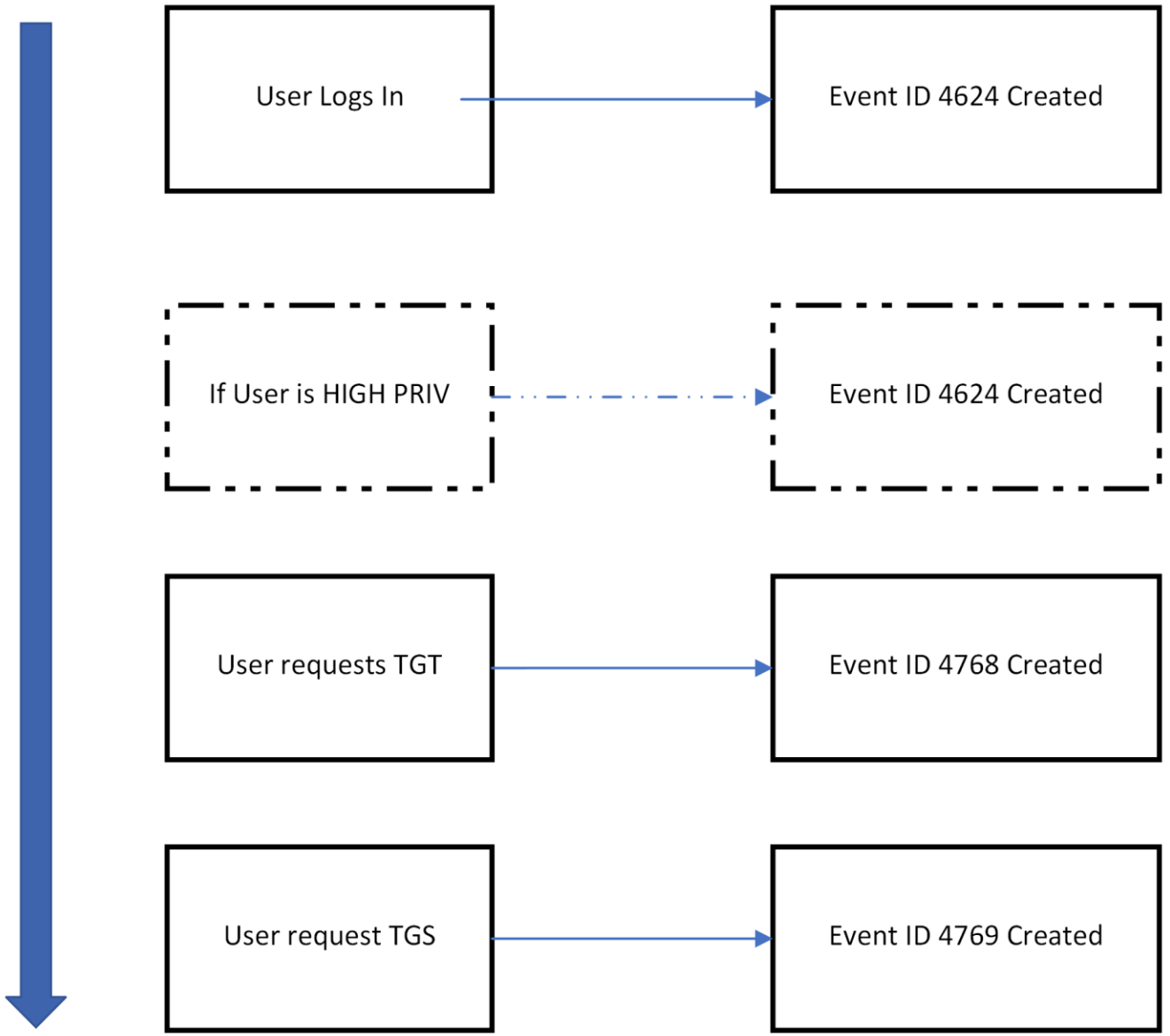
<u>Behaviors we will focus on:</u>

- Missing Auth Flow
- LOW PRIVs making 4672

Catching Golden Tickets: Missing Auth Flow

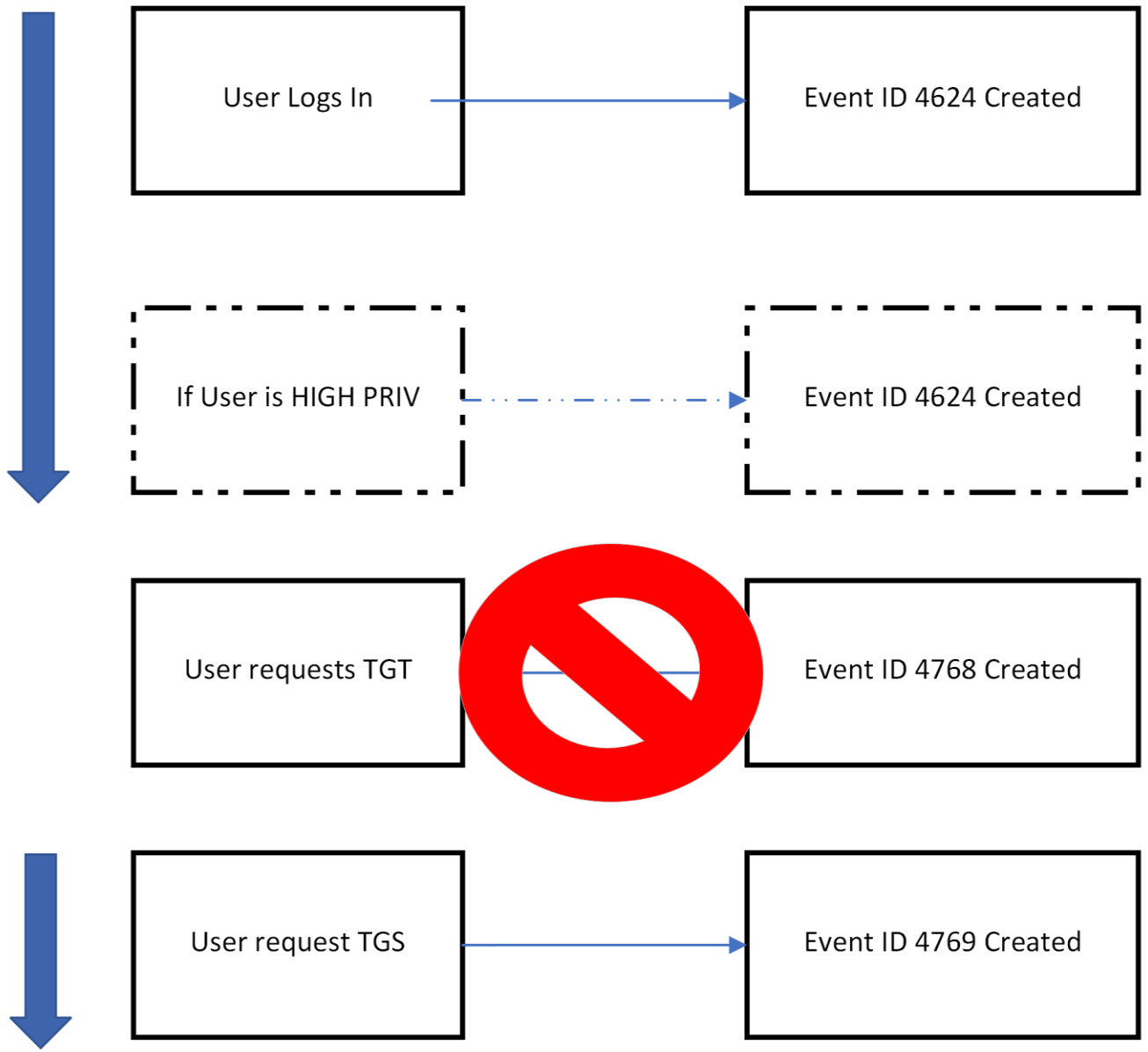
Event	4624 Logon
Event	4672 Special Logon (HIGH PRIV ACCOUNTS)
Event	4768 TGT request
Event	4769 TGS request

Normal Event Log Artifacts



G Ticket Event Log Artifacts

GOLDEN TICKET TRAFFIC FLOW

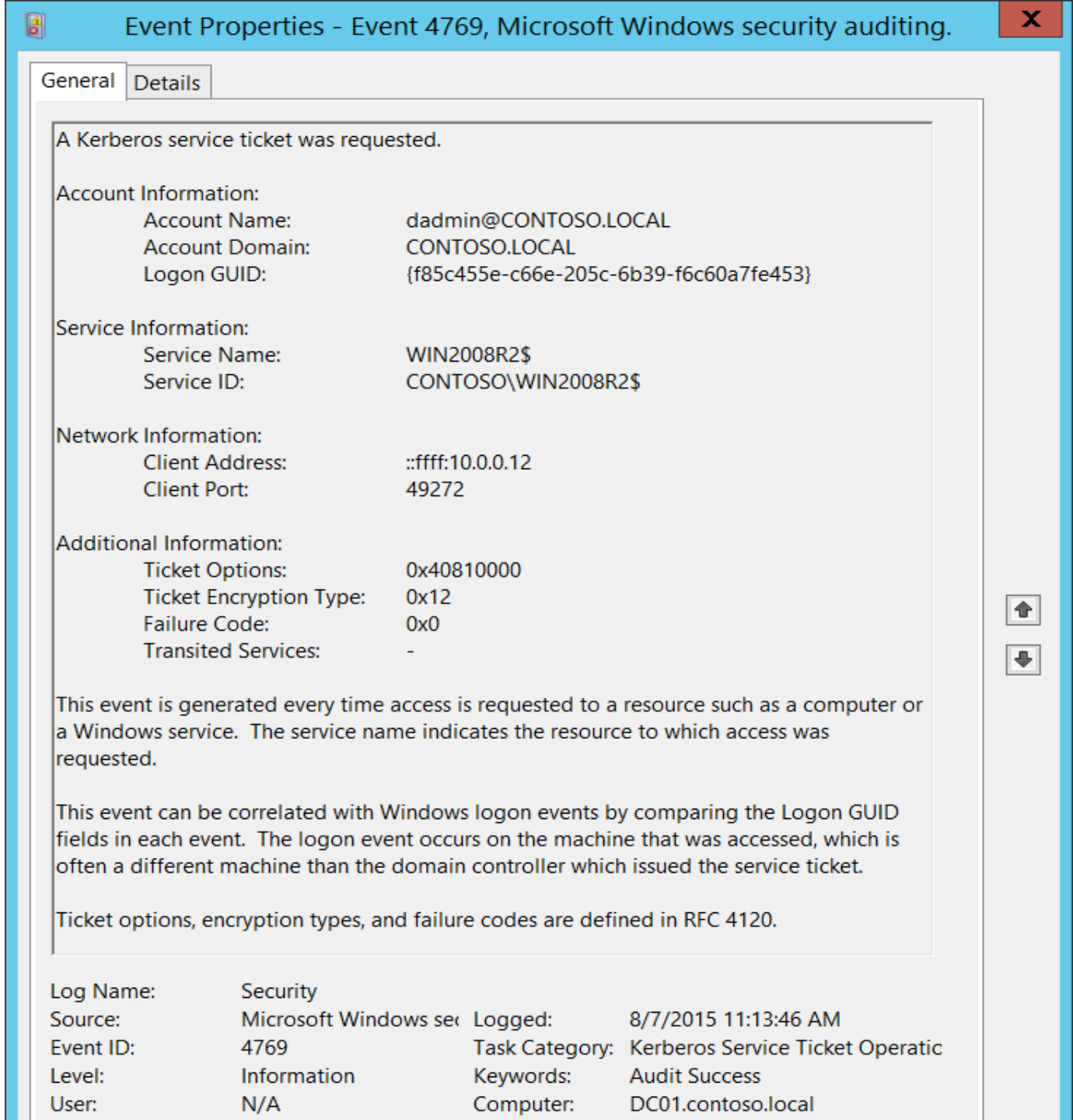


BrokeBoyz Cyber Kit™: Catching Kerberoasting

<u>Behaviors we will focus on:</u>

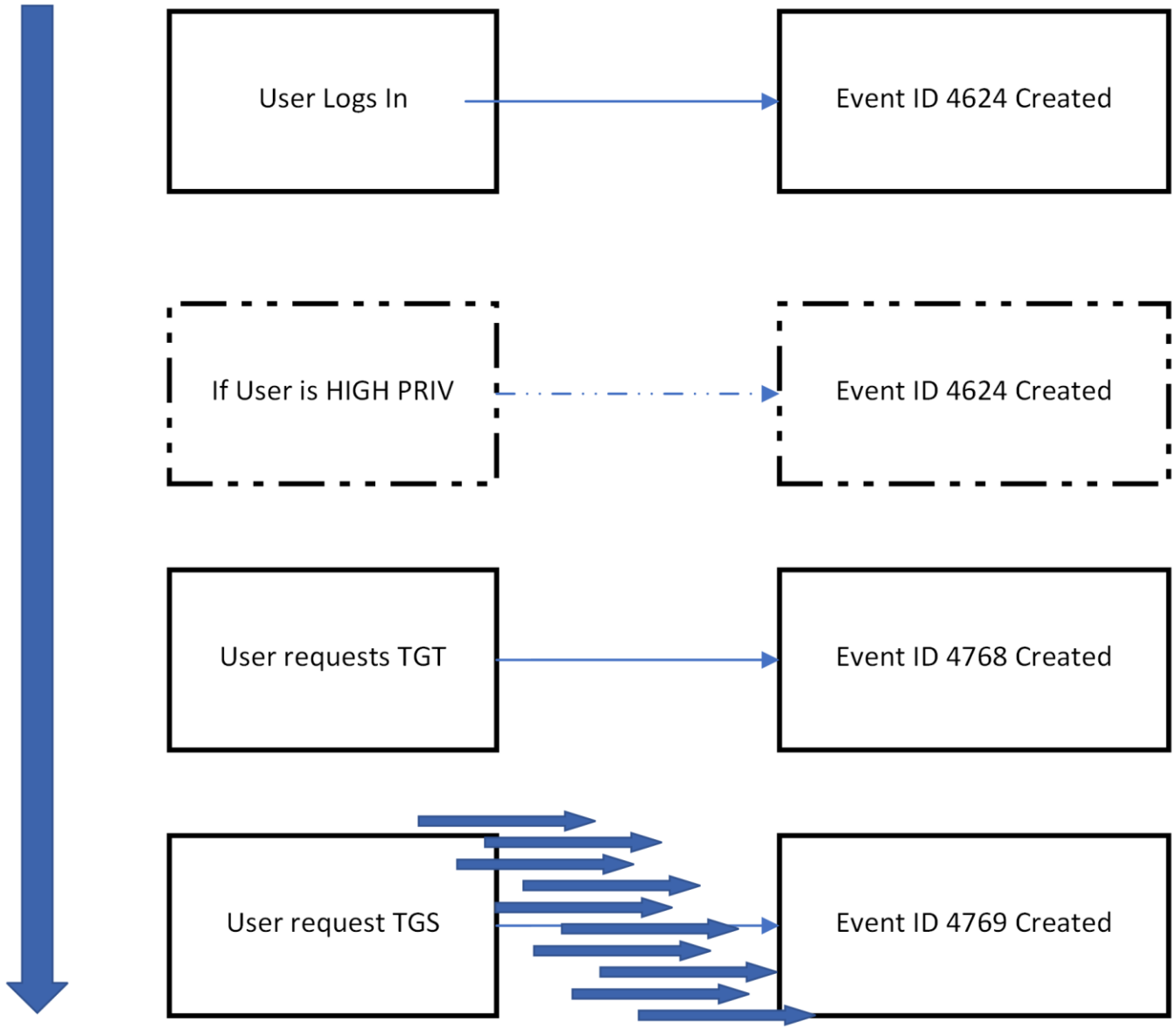
- Encryption downgrade (Default AES-256 Server 2016+)
- HIGH amounts of TGS request
- ~~Chad from Sales making TGS request to prod SQL SRVs~~

Catching Kerberoasting : Encryption Downgrade



<Level>0</Level>
<Task>14337</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2015-08-07T18:13:46.043256100Z" />
<EventRecordID>166746</EventRecordID>
<Correlation />
<Execution ProcessID="520" ThreadID="1496" />
<Channel>Security</Channel>
<Computer>DC01.contoso.local</Computer>
<Security />
</System>
- <EventData>
<Data Name="TargetUserName">dadmin@CONTOSO.LOCAL</Data>
<Data Name="TargetDomainName">CONTOSO.LOCAL</Data>
<Data Name="ServiceName">WIN2008R2$</Data>
<Data Name="ServiceSid">S-1-5-21-3457937927-2839227994-823803824-2102</Dat
<Data Name="TicketOptions">0x40810000</Data>
<Data Name="TicketEncryptionType">0x12</Data>
<Data Name="IpAddress">::ffff:10.0.0.12</Data>
<Data Name="IpPort">49272</Data>
<Data Name="Status">0x0</Data>
<Data Name="LogonGuid">{F85C455E-C66E-205C-6B39-F6C60A7FE453}</Data>
<Data Name="TransmittedServices">-</Data>
</EventData>
</Event>

Catching Kerberoasting: High TGS Request



Big thanks to

Johannes Pangrestu: Johannes Pangrestu, MBA | LinkedIn

Daniel Jimenez: Daniel López Jiménez | LinkedIn