SPECTEROPS

The Finer Details of LSA Credential Recovery

REcon 2025

Evan McBroom

SpecterOps

Introductions

- Systems developer
- On the “Internal and Community Products” team
- Special thanks to Benjamin Delpy 🥝

Problem Statement

Why do I care?

There are gaps in public documentation on LSA credential recovery.

- Logical abuses? Offline credential recovery? Mitigation technologies?
  - Lots of content! ✅
- Online credential recovery from user logon sessions?
  - “Read Mimikatz’s source code” ❌

Outline

What will you get?

- An intro to user logon sessions
- Memory scraping for credential recovery 🔑
- Credential Guard (and other mitigations) 🛡️
- Logical abuses for online credential recovery

Sources

Primary

- NT 3.5 – 5.2 sources
- NT 10 1607 x86 private PDBs
- NT 10 1703 ARM64 private PDBs
- Microsoft patents
- NT 10 22H2 – 24H2 PE modules

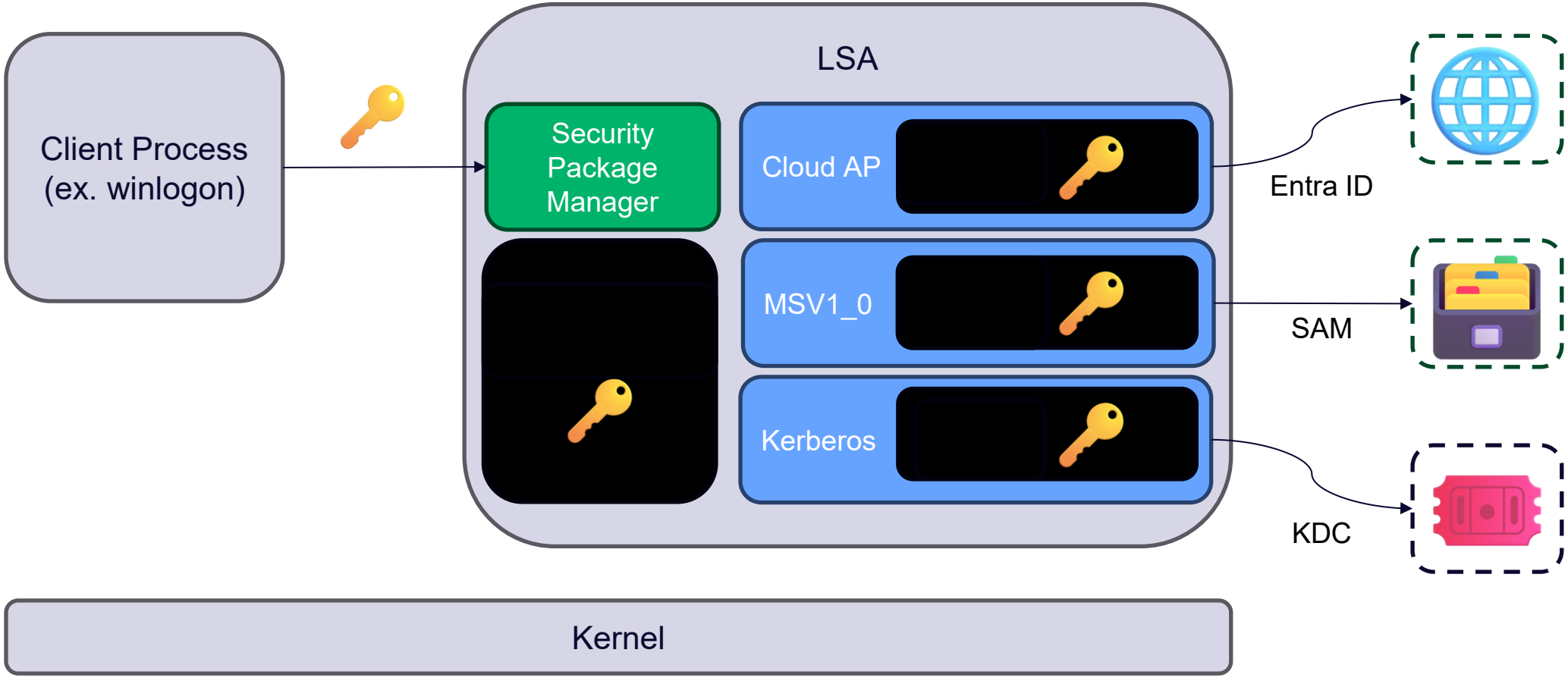
Secondary

- Mimikatz 🥝
- LSA Whisperer Development Kit (LWDK)
- Conference presentations

Windows Logon Sessions

Windows Logon Process

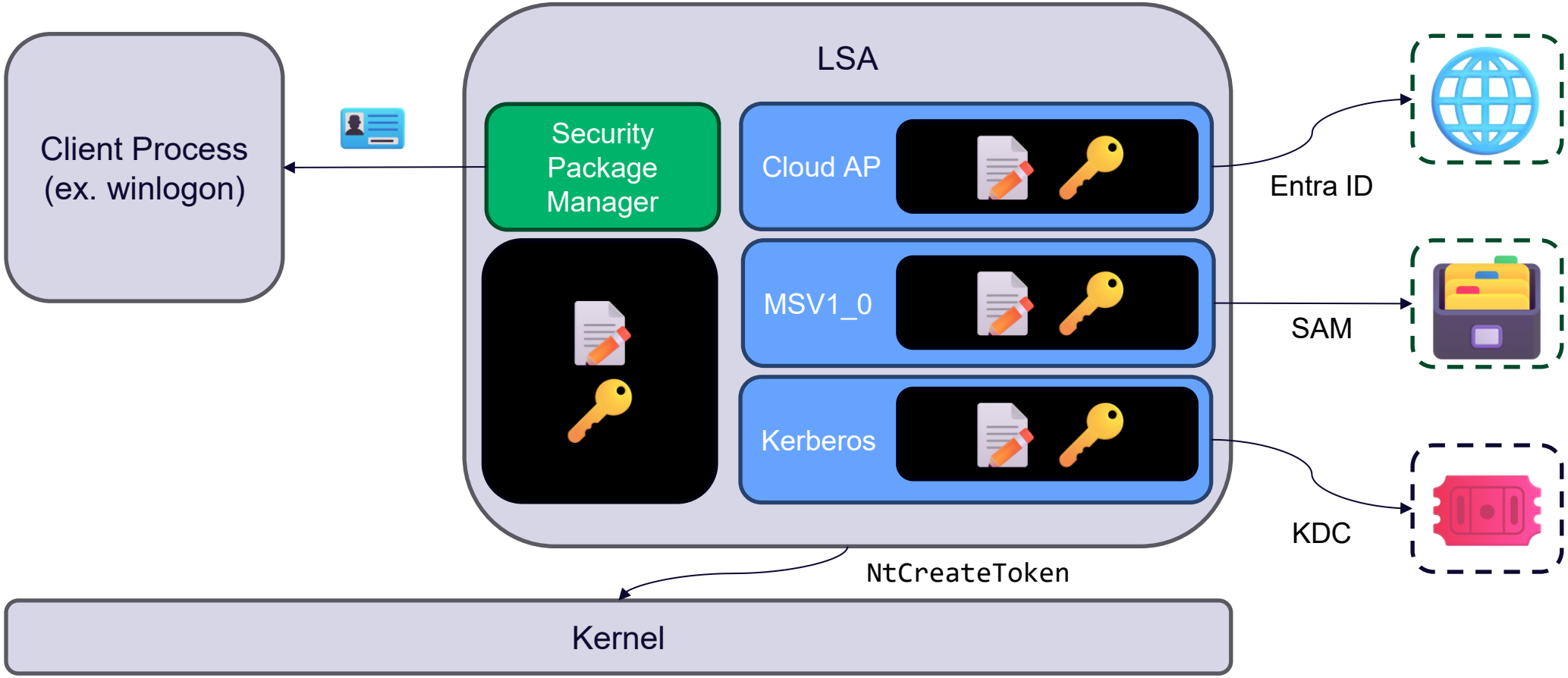
Authentication



Sources: NT 5.2 sources, NT 10 1607 and 1703 symbols, 24H2 modules

Windows Logon Process

Token Creation



Security Support Providers (SSPs)

Authentication Packages (APs)

1. Implement authentication logic
2. Maintains logon session information
3. Must implement at least one AP callback functions (ex. **LsaApLogonUser**)

~~**Security Packages (SPs)**~~

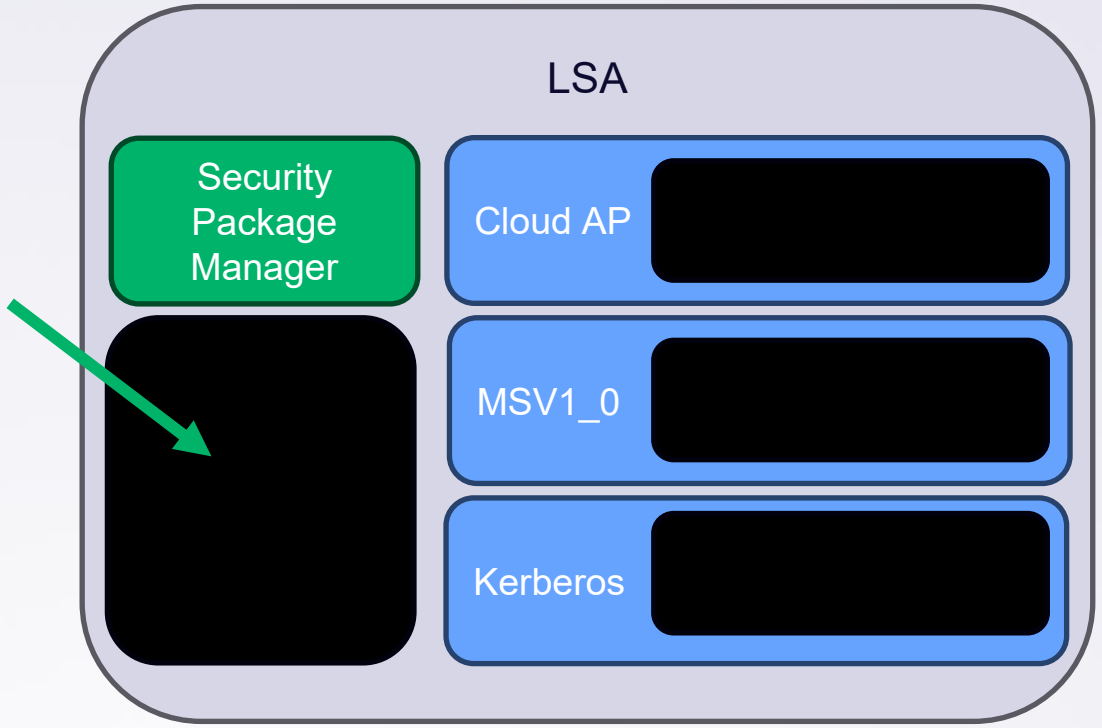
1. Implement a security protocol
2. Must implement at least one SP callback functions (ex. **SpAcceptCredentials**)

Source: https://learn.microsoft.com/en-us/windows/win32/secauthn/authentication-functions

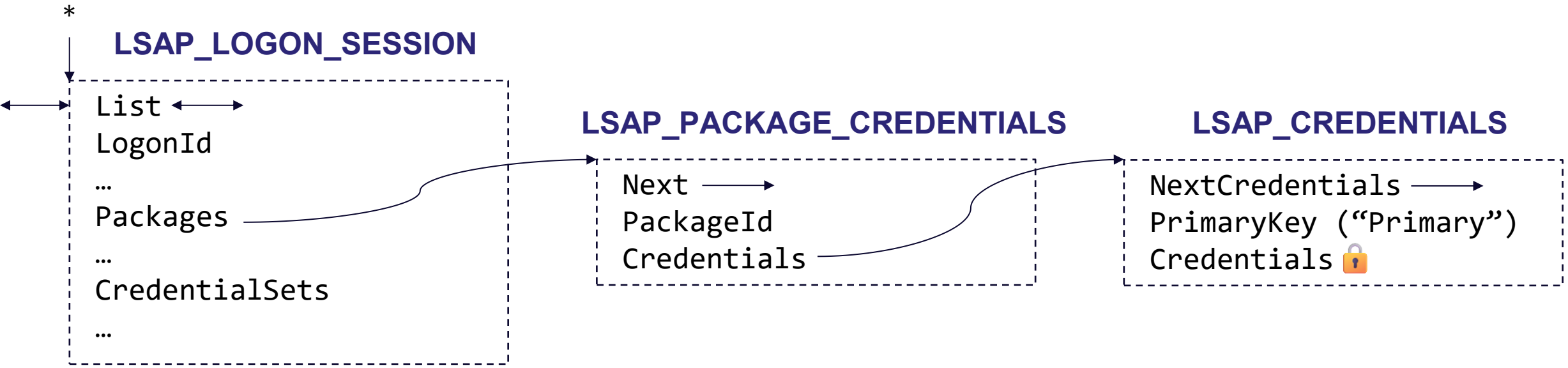
Dll	Common Name	SP	AP	RPC ID	RPC Authn
cloudap	Cloud AP	OAuth 2.0	✓	36	`CLOUD_AP`
credssp	Credential Delegation SSP	TLS+SPNEGO	—		
kerberos	Kerberos	Kerberos	✓	16	`GSS_KERBEROS`
livessp	Live SSP	?	✓	32	`LIVE_SSP`
msapsspc	DPA Client	RPA	—	17	`DPA`
msnsspc	MSN Client	NTLM	—	18	`MSN`
msv1_0	Microsoft Authentication Package v1.0	NTLM	✓	10	`WINNT`
negoexts	Negotiate Extender	NEGOEX	✓	30	`NEGO_EXTENDER`
negotiate	Negotiate	SPNEGO	✓	9	`GSS_NEGOTIATE`
pku2u	Public Key User to User	PKU2U	✓	31	`NEGO_PKU2U`
schannel	Secure Channel	SSL/TLS	✓	14	`GSS_SCHANNEL`
tspkg	Terminal Services Package		✓	22	?
wdigest	Windows Digest	Digest Access	✓	21	`DIGEST`

Source: LSA Whisperer wiki

Memory Scraping


LSA
Security Package Manager
Cloud AP
MSV1_0
Kerberos

LSA Logon Session List



*maintained by the lsa server

MSV1_0 Primary Credentials

Old Design

Original

MSV1_0_PRIMARY_CREDENTIAL

```
LogonDomainName
UserName
NtOwfPassword
LmOwfPassword
…
```

XP

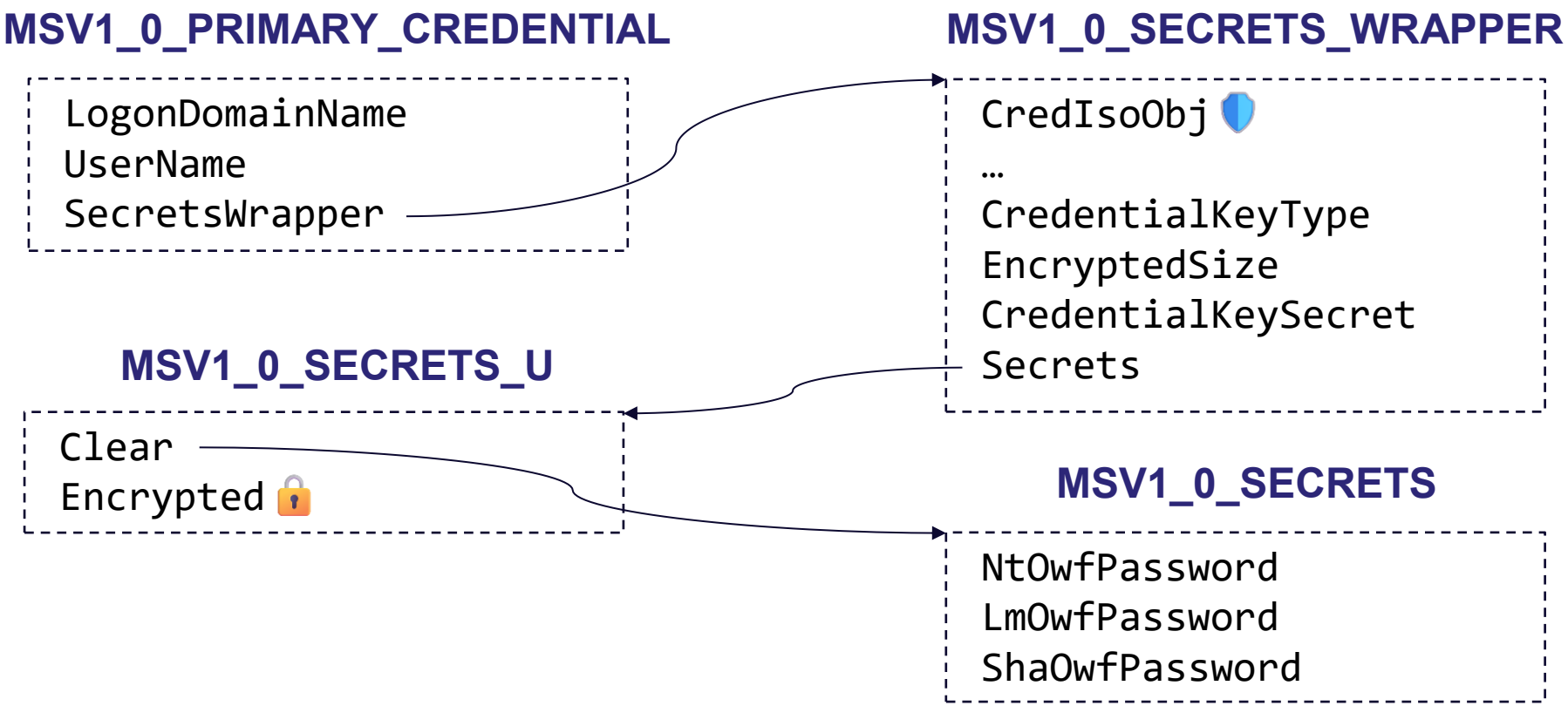
MSV1_0_PRIMARY_CREDENTIAL

```
LogonDomainName
UserName
NtOwfPassword
LmOwfPassword
ShaOwfPassword
…
```

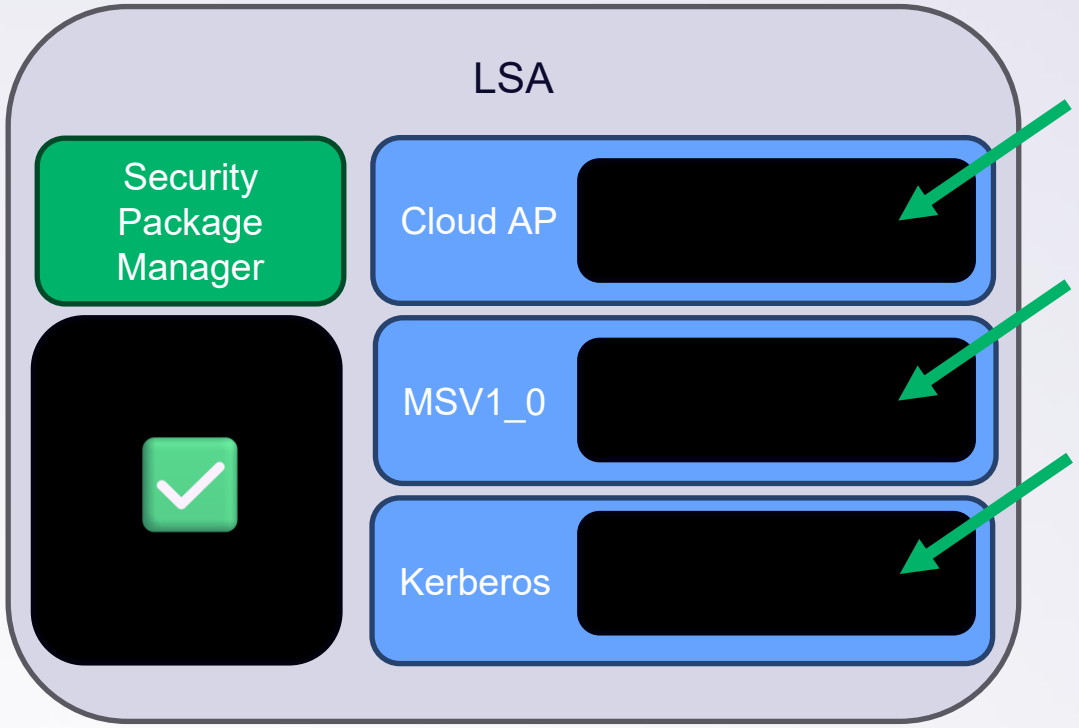

Sources: NT 5.2 and prior sources

MSV1_0 Primary Credentials

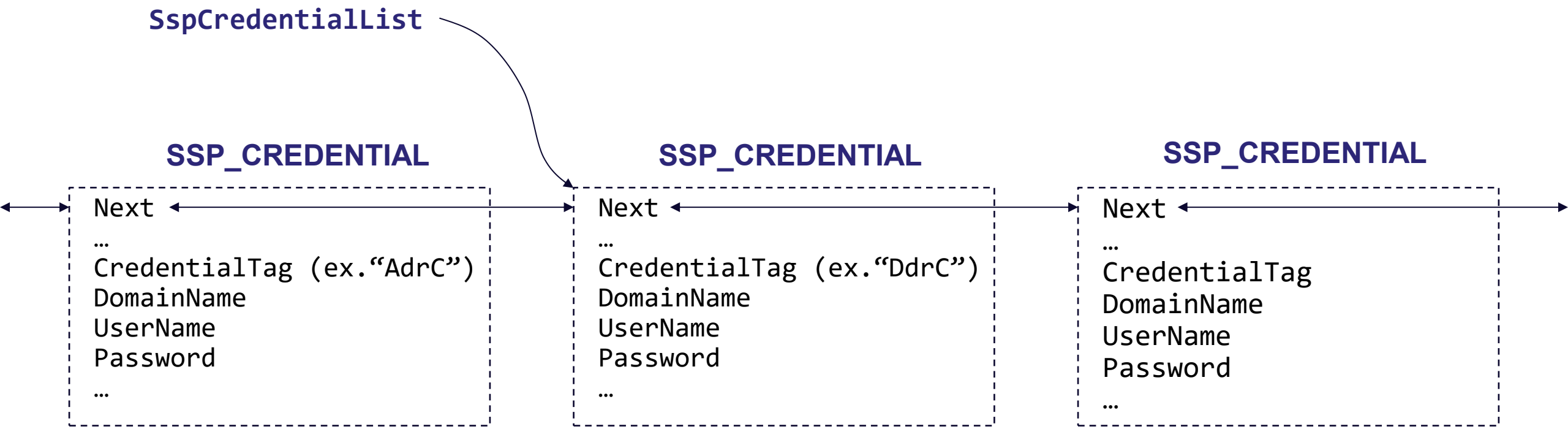
New Design (1607)



Source: LWDK


LSA
Security Package Manager
Cloud AP
MSV1_0
Kerberos

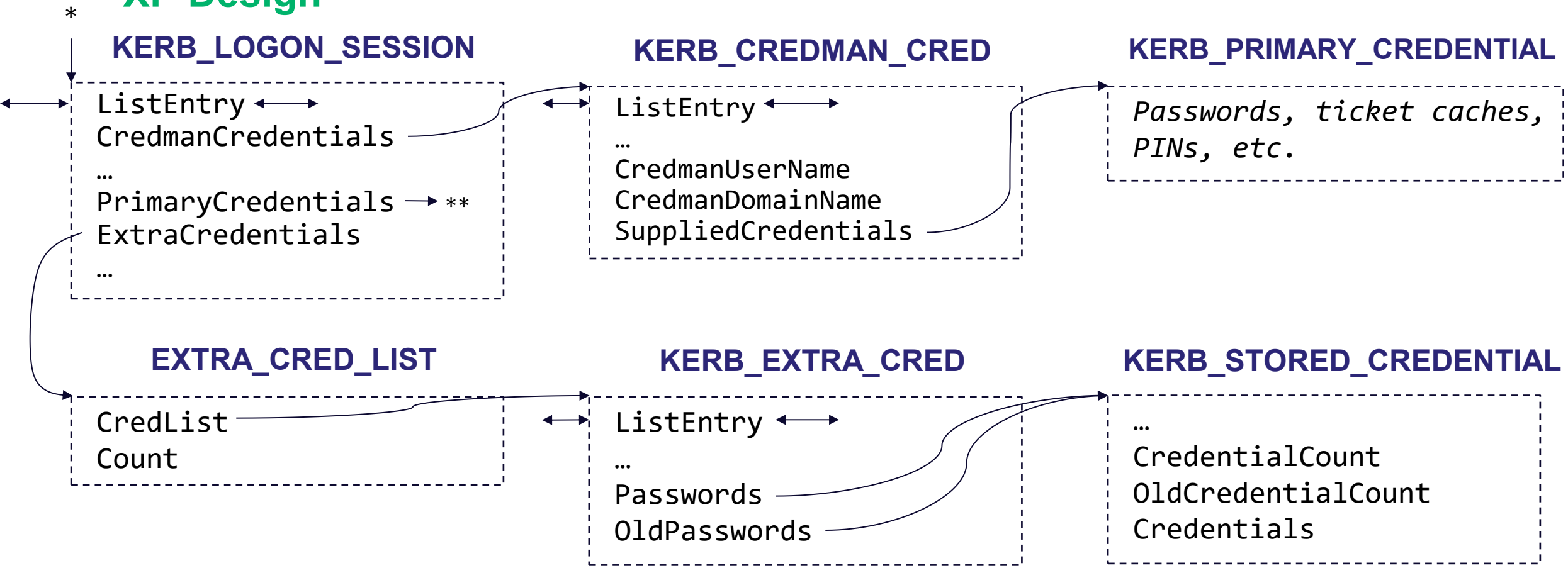
MSV1_0 Credential List



Sources: NT 5.2 sources, and NT 10 1607 and 1703 symbols

Kerberos Logon Session List

XP Design



**Also KERB_PRIMARY_CREDENTIAL

Source: NT 5.2 sources

Kerberos Logon Session Table

Vista+ Design

*

KERB_LOGON_SESSION

References
CredmanCredentials
…
PrimaryCredentials → **
ExtraCredentials
…

KERB_CREDMAN_CRED

ListEntry ↔
…
CredmanUserName
CredmanDomainName
SuppliedCredentials

KERB_PRIMARY_CREDENTIAL

Passwords, ticket caches, PINs, etc.
…
Kdc supplied keys, packed credentials, kdc proxy caches, s4u2proxy caches

EXTRA_CRED_LIST

CredList
Count

KERB_EXTRA_CRED

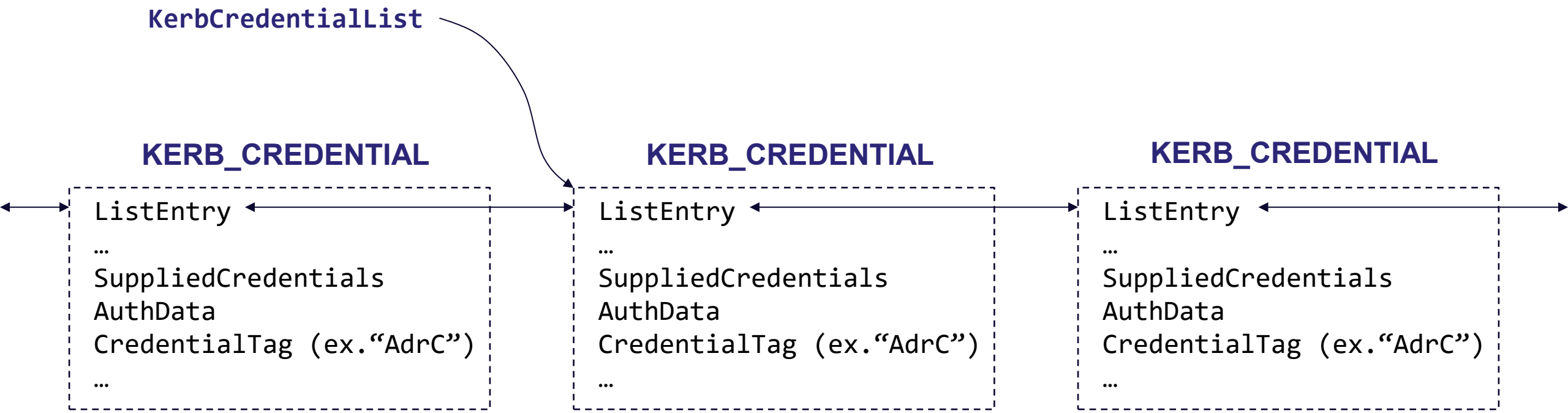
ListEntry ↔
…
SuppliedCredentials
…

KERB_STORED_CREDENTIAL

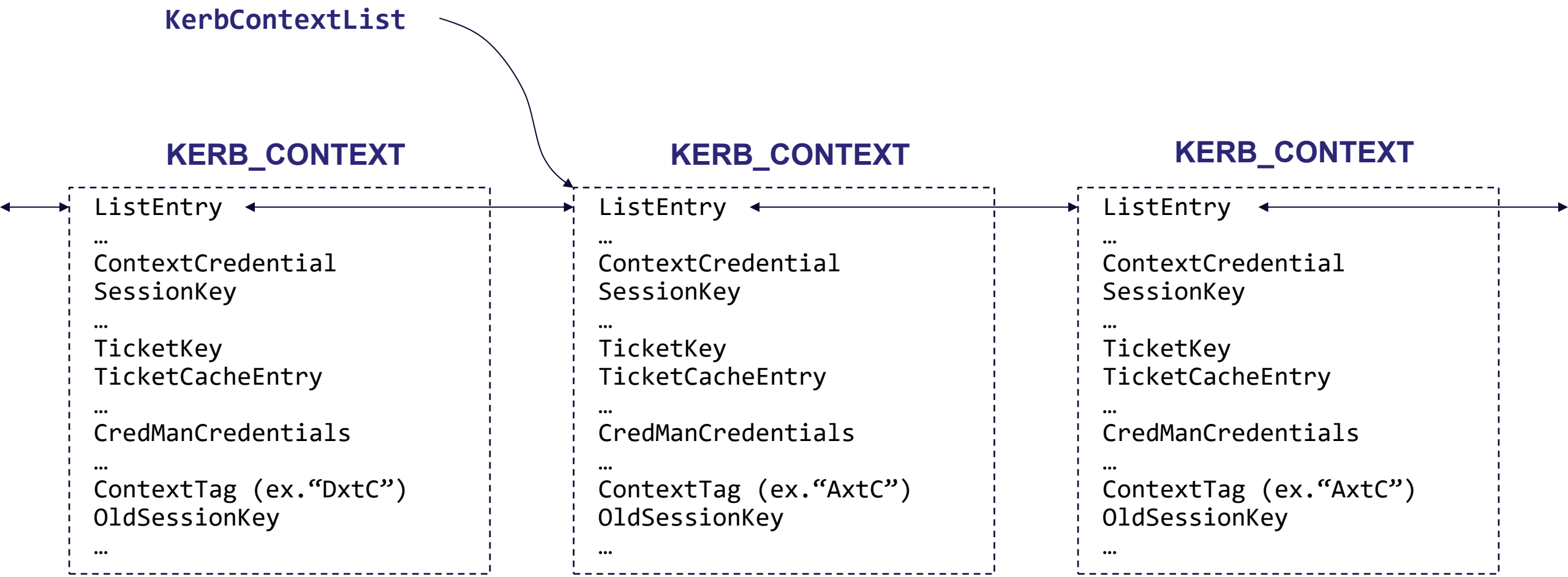
…
Current, old, "older", and service credential counts
…
Credentials

**Also KERB_PRIMARY_CREDENTIAL

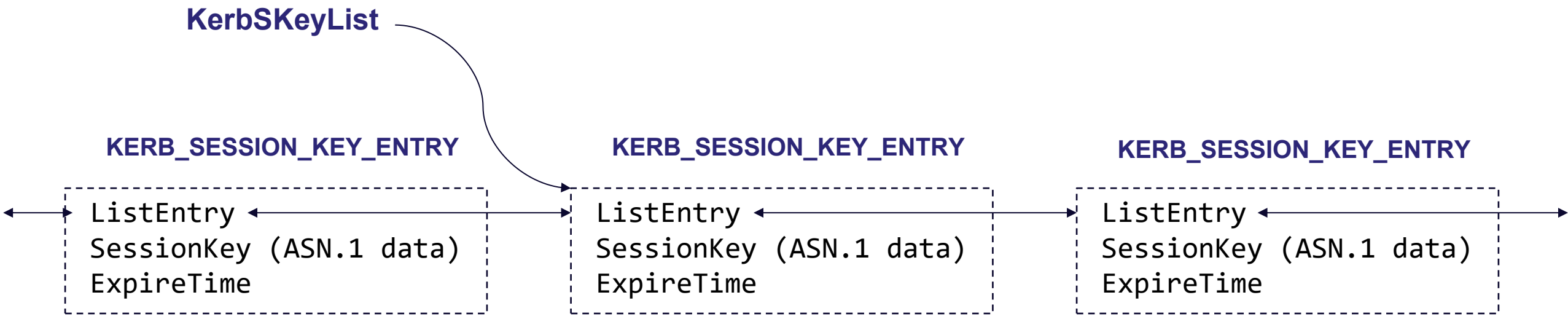
Kerberos Credential List



Kerberos Context List



Kerberos Session Key List



PKU2U Logon Sessions

Note: all type names are prefixed with **PKU2U_**.

*

LOGON_SESSION

```
Signature ("PKUUSESS")
…
AssociatedCredentials
```

CONTEXT

```
Signature ("PKUUATXT")
…
ContextCredential
CredmanCredential
AssociatedCredential
…
TicketCacheEntry**
SessionKey
TicketKey
```

ASSOCIATED_CREDENTIAL

```
ListEntry
Signature ("PKUUASCD")
…
PrimaryCredential
```

SECONDARY_CREDENTIAL

```
Signature ("PKUUCRED")
…
CredentialKey
PrimaryCredential
```

PRIMARY_CREDENTIAL

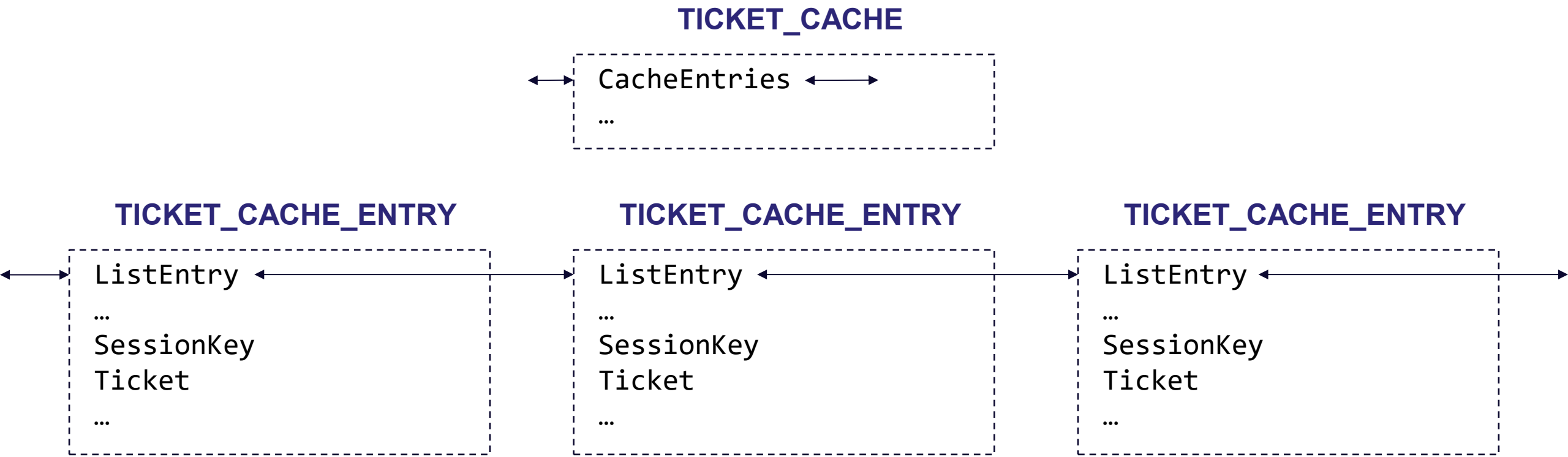
```
…
ServerTicketCache**
…
Peer2PeerKeyCount
Peer2PeerKeys
```

*Pku2uGlobalLogonSessionTable

**on next slide

PKU2U Ticket Cache

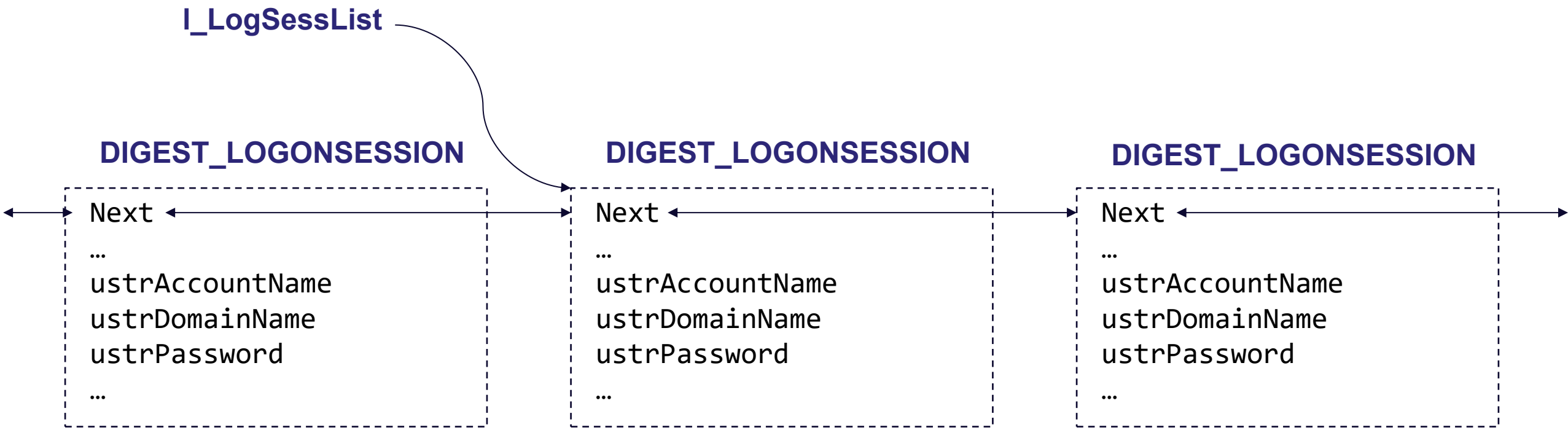
Note: all type names are prefixed with **PKU2U_**.



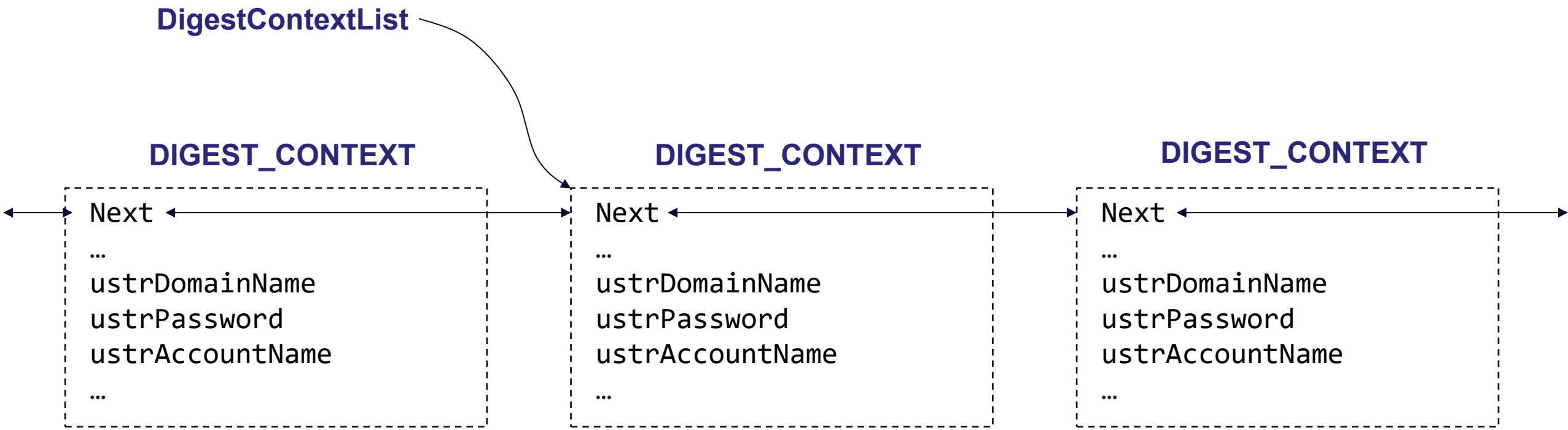
PKU2U Credential Table

Note: all type names are prefixed with **PKU2U_**.

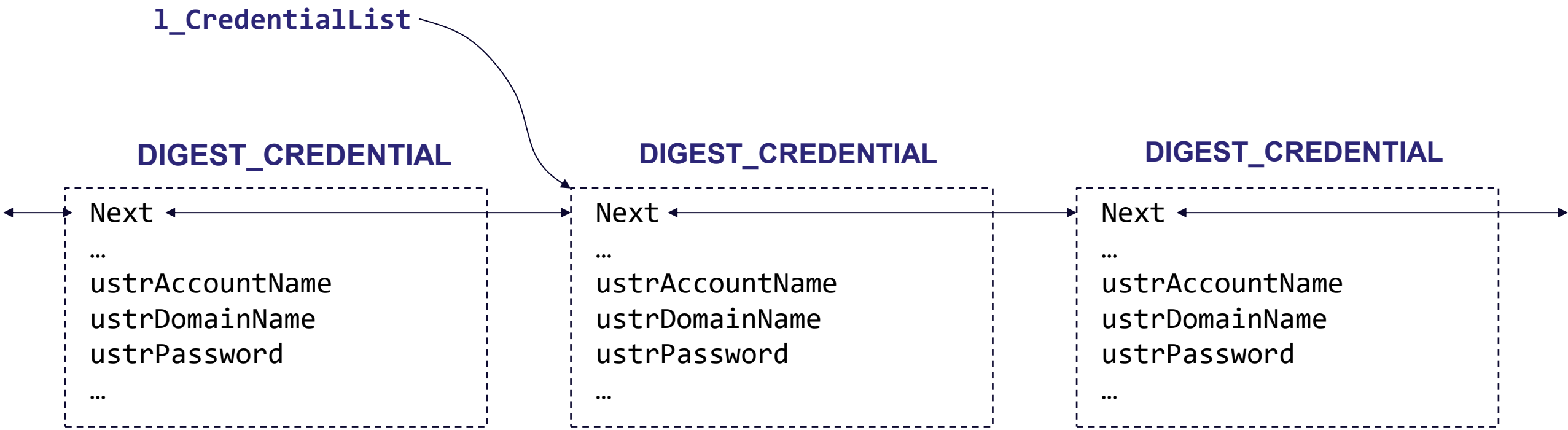
WDigest Logon Sessions



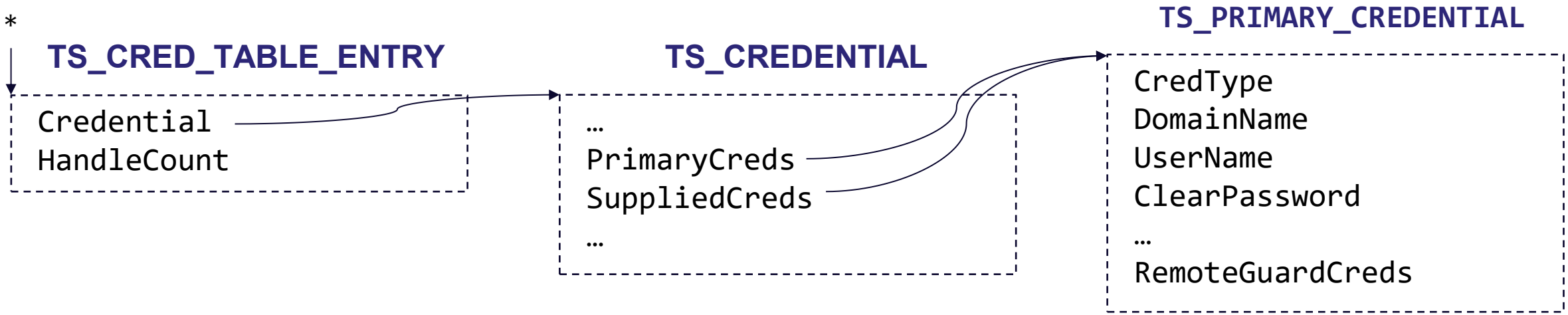
WDigest Context Lists



WDigest Credential Lists



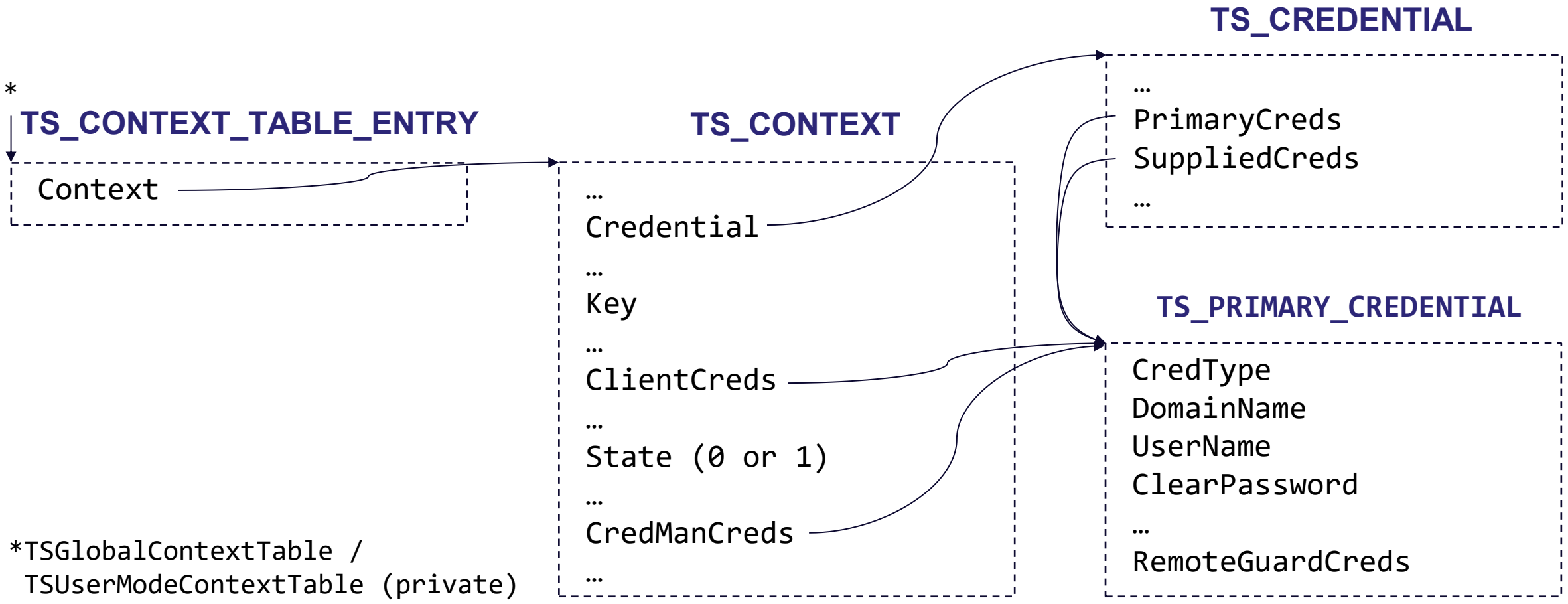
TsPkg Credential Table



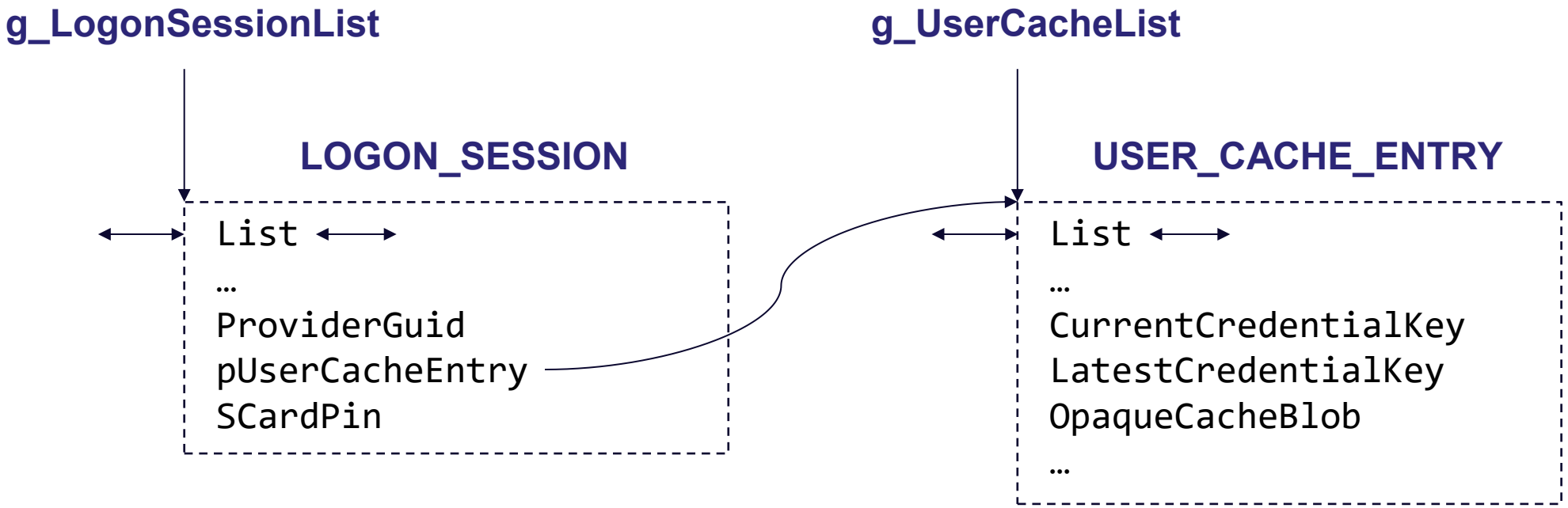
*TSGlobalCredTable

Sources: NT 10 1607 and 1703 symbols, LWDK, 24H2 modules, Mimikatz

TsPkg Context Table



CloudAP Logon Sessions



Sources: NT 10 1607 and 1703 symbols, 24H2 modules, Mimikatz

Credential Scorecard

cloudap

Credential keys
Plugin data:
- PRTs
- Session keys

Smart card PIN data

kerberos

Plaintext passwords
CredMan credentials
TGTs & Session Keys
TGSs & Session Keys
Encryption keys
Smart card PIN data

msv1_0

Plaintext passwords
CredMan credentials
OWFs (LM / NT / SHA)
Secure Credential Keys

pku2u

CredMan credentials
Tickets
Session keys
P2P keys

tspkg

Plaintext passwords
CredMan credentials

wdigest

Plaintext passwords

Memory Scraping

Just the Highlights

- Most package structures are stable (exc. Vista, 10 1607, CloudAP)
- Symbols and magic values can remove the need for byte signatures
- More credential recovery potential exists than what Mimikatz implements

Credential Guard

(and other mitigations 🙂)

Credential Guard

Just the Highlights

- Officially supported on Windows Education/Enterprise*
- Protects credentials for MSV1_0 and Kerberos logon sessions
- Inputted credentials are stored in a “VM” and not directly accessible
- Limits the operations that can be performed on protected credentials

Source: “Unguarding Microsoft Credential Guard | SO-CON 2025” – Ceri Coburn

Credential Guard APIs

NtlmCredIso[Api/InProc/Ium]

```
CalculateNtResponse
CalculateUserSessionKeyNt
Compare[Credentials/...]
DecryptDpapiMasterKey
EncodeCredManPasswordAsNtlmIumPassword
EncodePasswordAsSupplementalCredential
GenerateRootSecret
GetCredentialKey
Lm20GetNtlm3ChallengeResponse
MakeSecretPasswordNT5
PasswordValidate[Interactive/Network]
ProtectCredential
ProtectSspCredentialPassword
UpdateSharedConfiguration
...
```

KerbCredIso[Api/InProc/Ium]

```
AreEncrypt[edBuffers/ionKeys]Equal
Build[EncryptedAuthData/...]
ComputeTgsChecksum
Create[Ap/As]ReqAuthenticator
Create[DH/ECDH]KeyAgreement
Decrypt[ApReply/PacCredentials/...]
EncodeCredManPasswordAsKerbPassword
GetNtlmSupplementalCredential
[Hash/Sign]S4UPreauth[Data]
PackApReply
SecureDuplicatePassword
UnpackKdcReplyBody
UpdateSharedConfiguration
Verify[Checksum/ServiceTicket/...]
...
```


Sources: NT 10 1607 and 1703 symbols, 24H2 modules

Credential Guard Restricted Operations

MSV1_0

- MK encryption key retrieval
- SHA OWF retrieval
- NTLMv1 response generation

Kerberos

- DES encryption
- TGT session key retrieval
- Unconstrained delegation

Sources: “LSA Whisperer | SO-CON 2024” – Evan McBroom, LSA Whisperer wiki

Credential Scorecard 📝 (+ Credential Guard)

cloudap

Credential keys
Plugin data:
- PRTs
- Session keys

Smart card PIN data

kerberos

~~Plaintext passwords~~
~~CredMan credentials~~
TGTs & ~~Session Keys~~
TGSs & Session Keys
~~Encryption keys~~
~~Smart card PIN data~~

msv1_0

~~Plaintext passwords~~
~~CredMan credentials~~
~~OWFs (LM / NT / SHA)~~
~~Secure Credential Keys~~

pku2u

CredMan credentials
Tickets
Session keys
P2P keys

tspkg

Plaintext passwords
CredMan credentials

wdigest

Plaintext passwords

Sources: https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/how-it-works#credential-guard-protection-limits

Other Mitigations

- WDigest disablement
- LSA Protection
  - LSA executes as a Protected Process Light
  - Adds signing requirements for LSA plugins
- Remote Credential Guard
- TPM usage for credential storage
- “NTLMv1 removal” 🫠
- Password removal from MPR notifications

Sources: https://learn.microsoft.com/en-us/windows/whats-new/

Credential Scorecard 📝 (+ WDigest disabled)

cloudap

Credential keys
Plugin data:
- PRTs
- Session keys

Smart card PIN data

kerberos

~~Plaintext passwords~~
~~CredMan credentials~~
TGTs & ~~Session Keys~~
TGSs & Session Keys
~~Encryption keys~~
~~Smart card PIN data~~

msv1_0

~~Plaintext passwords~~
~~CredMan credentials~~
~~OWFs (LM / NT / SHA)~~
~~Secure Credential Keys~~

pku2u

CredMan credentials
Tickets
Session keys
P2P keys

tspkg

Plaintext passwords
CredMan credentials

wdigest

~~Plaintext passwords~~

Credential Scorecard 📝 (+ LSA protection)

cloudap

~~Credential keys~~
~~Plugin data:~~
- ~~PRTs~~
- ~~Session keys~~

~~Smart card PIN data~~

kerberos

~~Plaintext passwords~~
~~CredMan credentials~~
TGTs & ~~Session Keys~~
TGSs & Session Keys
~~Encryption keys~~
~~Smart card PIN data~~

msv1_0

~~Plaintext passwords~~
~~CredMan credentials~~
~~OWFs (LM / NT / SHA)~~
~~Secure Credential Keys~~

pku2u

~~CredMan credentials~~
~~Tickets~~
~~Session keys~~
~~P2P keys~~

tspkg

~~Plaintext passwords~~
~~CredMan credentials~~

wdigest

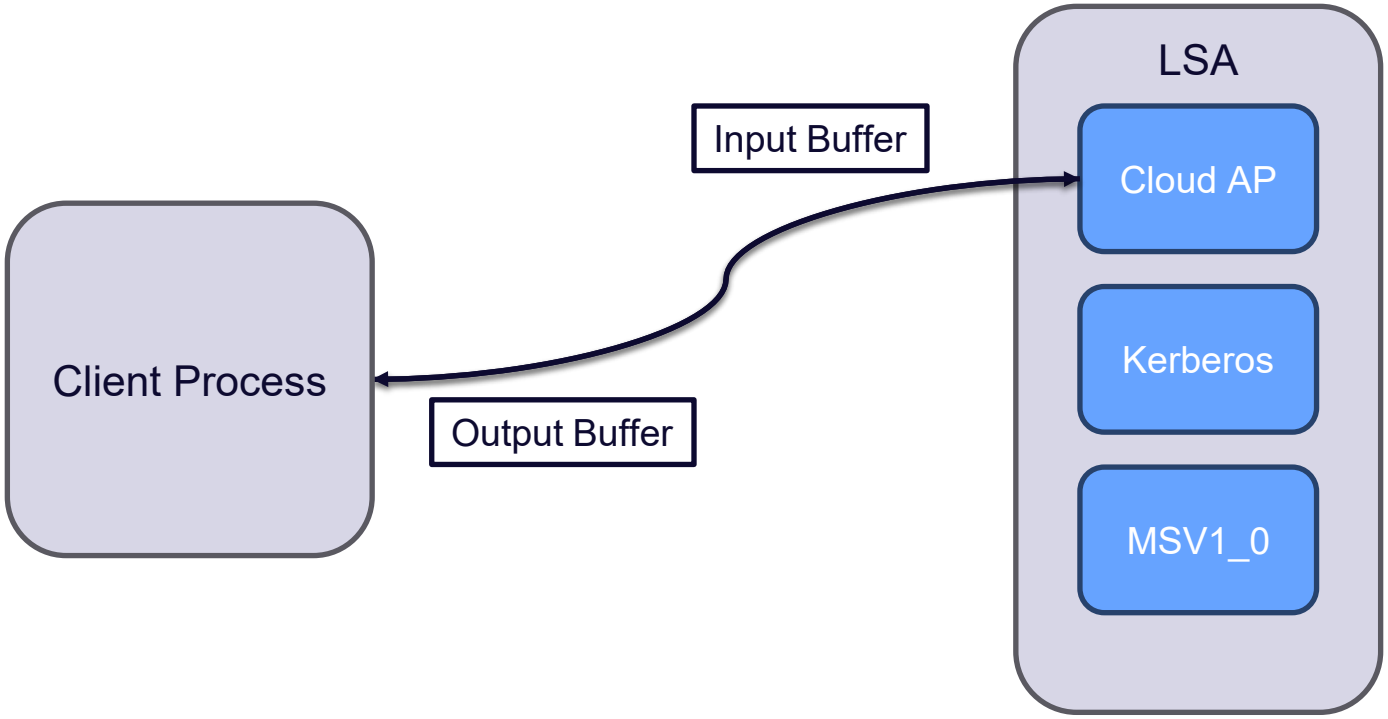
~~Plaintext passwords~~

Logical Abuses

Easy to Use, Hard to Fix

Authentication Package Calls

LsaCallAuthenticationPackage



Authentication Package Calls

For Credential Recovery

cloudap	CreateDeviceSSOCookie CreateEnterpriseSSOCookie CreateSSOCookie GetSignedProofOfPossessionTokens	SSO Cookies
kerberos	RetrieveEncodedTicket RetrieveTicket	TGTs & ~~Session Keys~~ TGSs & Session Keys
msv1_0	GetCredentialKey GetStrongCredentialKey Lm20GetChallengeResponse	OWFs (NT / SHA)* Secure Cred Keys* NTLMv1 Responses

Credential Scorecard

cloudap

~~Credential keys~~
~~Plugin data:~~
- ~~PRTs~~
- ~~Session keys~~

~~Smart card PIN data~~

kerberos

~~Plaintext passwords~~
~~CredMan credentials~~
TGTs & ~~Session Keys~~
TGSs & Session Keys
~~Encryption keys~~
~~Smart card PIN data~~

msv1_0

~~Plaintext passwords~~
~~CredMan credentials~~
~~OWFs (LM / NT / SHA)~~
~~Secure Credential Keys~~

pku2u

~~CredMan credentials~~
~~Tickets~~
~~Session keys~~
~~P2P keys~~

tspkg

~~Plaintext passwords~~
~~CredMan credentials~~

wdigest

~~Plaintext passwords~~

Credential Scorecard 📝 (+ active logon sessions)

cloudap

~~Credential keys~~
~~Plugin data:~~
- ~~PRTs~~
- ~~Session keys~~
- SSO cookies
~~Smart card PIN data~~

kerberos

~~Plaintext passwords~~
~~CredMan credentials~~
TGTs & ~~Session Keys~~
TGSs & Session Keys
~~Encryption keys~~
~~Smart card PIN data~~

msv1_0

~~Plaintext passwords~~
~~CredMan credentials~~
OWFs (~~LM~~ / NT / SHA)
Secure Credential Keys
NTLMv1 Responses*

pku2u

~~CredMan credentials~~
~~Tickets~~
~~Session keys~~
~~P2P keys~~

tspkg

~~Plaintext passwords~~
~~CredMan credentials~~

wdigest

~~Plaintext passwords~~

Other Abuses

- Gather credentials stored elsewhere:
  - Account databases: Registry hives, NTDS.dit
  - Password storage: Credential Store, Vault, NGC data, 3rd party applications
  - File systems: attached devices, mounted volumes, volume shadow copies, VHDs, VMDKs
- Bypass LSA protection (ex. load a module)
- Bypass Credential Guard logic (ex. obfuscate the TGT SPN)
- Indirectly access memory (ex. PCIe, VMRSs, VMSNs)
- Indirectly access user inputs (ex. key logging)

Credential Scorecard

cloudap

~~Credential keys~~
~~Plugin data:~~
- ~~PRTs~~
- ~~Session keys~~
- SSO cookies

~~Smart card PIN data~~

kerberos

~~Plaintext passwords~~
~~CredMan credentials~~
TGTs & ~~Session Keys~~
TGSs & Session Keys
~~Encryption keys~~
~~Smart card PIN data~~

msv1_0

~~Plaintext passwords~~
~~CredMan credentials~~
OWFs (~~LM~~ / NT / SHA)
Secure Credential Keys
NTLMv1 Responses*

pku2u

~~CredMan credentials~~
~~Tickets~~
~~Session keys~~
~~P2P keys~~

tspkg

~~Plaintext passwords~~
~~CredMan credentials~~

wdigest

~~Plaintext passwords~~

Credential Scorecard 📝 (+ PPL bypass)

cloudap

Credential keys
Plugin data:
- PRTs
- ~~Session keys~~
- SSO cookies

Smart card PIN data

kerberos

~~Plaintext passwords~~
~~CredMan credentials~~
TGTs & ~~Session Keys~~
TGSs & Session Keys
~~Encryption keys~~
~~Smart card PIN data~~

msv1_0

~~Plaintext passwords~~
~~CredMan credentials~~
OWFs (~~LM~~ / NT / SHA)
Secure Credential Keys
NTLMv1 Responses*

pku2u

CredMan credentials
Tickets
Session keys
P2P keys

tspkg

~~Plaintext passwords~~
~~CredMan credentials~~

wdigest

~~Plaintext passwords~~

Credential Scorecard 📝 (+ CG logic bypass)

cloudap

Credential keys
Plugin data:
- PRTs
- ~~Session keys~~
- SSO cookies

Smart card PIN data

kerberos

~~Plaintext passwords~~
~~CredMan credentials~~
TGTs & Session Keys
TGSs & Session Keys
~~Encryption keys~~
~~Smart card PIN data~~

msv1_0

~~Plaintext passwords~~
~~CredMan credentials~~
OWFs (~~LM~~ / NT / SHA)
Secure Credential Keys
NTLMv1 Responses*

pku2u

CredMan credentials
Tickets
Session keys
P2P keys

tspkg

~~Plaintext passwords~~
~~CredMan credentials~~

wdigest

~~Plaintext passwords~~

Credential Scorecard

cloudap

Credential keys
Plugin data:
- PRTs
- ~~Session keys~~
- SSO cookies

Smart card PIN data

kerberos

~~Plaintext passwords~~
~~CredMan credentials~~
TGTs & Session Keys
TGSs & Session Keys
~~Encryption keys~~
~~Smart card PIN data~~

msv1_0

~~Plaintext passwords~~
~~CredMan credentials~~
OWFs (~~LM~~ / NT / SHA)
Secure Credential Keys
NTLMv1 Responses*

pku2u

CredMan credentials
Tickets
Session keys
P2P keys

tspkg

~~Plaintext passwords~~
~~CredMan credentials~~

wdigest

~~Plaintext passwords~~

Epilogue

Wrap-Up

One less public documentation gap on LSA credential recovery ✅

- Scraping credentials from LSA memory is not too difficult
- Credential Guard and other mitigations are not too scary
- Defenders → still update to Windows 11 24H2 and enable mitigations
- Microsoft → incorporate pku2u into Credential Guard

Reference: https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/credentials-protection-and-management

SPECTEROPS

Questions?

Evan McBroom | emcbroom@specterops.io
| evanmcbroom.bsky.social

SPECTEROPS

Thank you!

Evan McBroom | emcbroom@specterops.io
| evanmcbroom.bsky.social