IPAM Security Considerations

N3K Expert Webinar Series

Andreas Taudte
Principal DDI Consultant

Last updated August 2023

Housekeeping

- Timing, Schedule, Q&A Session
- Online Etiquette (microphones, distracting activities)
- Recording and Privacy

Accessing the Infrastructure

- Web UIs and APIs encrypted with SSL (HTTPS) and CLIs encrypted with SSH
- Admin Access via internal or VPN Networks (Zero Trust!?)
- Direct Machine Access reserved for Core Team
  - SSH Console Access
  - Hardware, out-of-band Management and Hypervisor Console Access
  - Lab and Consolidation Environments
- Reasonable UI Session Timeout (e.g. 2 hours)
- Dependability of the Infrastructure
  - Restricted File System Access to minimal Individuals
  - Disabled non-essential Protocols by Design (e.g. no DHCP on DNS-only system)
- Establishment of Jump Servers to access Infrastructure Components

Data within the Infrastructure

- Data Exchange over corporate Networks (Zero Trust!?)
- Only essential Data collected for Functionality
- Database Objects with User Action Audit Trails
- Archive Transaction & Event History (e.g. 6 months)
- Track User Sessions with Name, IP, Time and State

Classification of User Accounts

- Account Creation Issues: on-demand with no Validation, many overprivileged Accounts
- Need for role-based Classification based on Experience and Role
- Core Team has both full-access and reduced-access Accounts
  - Use reduced Access for daily Tasks (like an operator account)
  - Full Access only for essential administrative Tasks like System Changes

User Classes & Access Rights

- IPAM Users
  - Basic DNS and DHCP Tasks
  - Access after Application via Approval Process
- IPAM Operators
  - Advanced DNS and DHCP Tasks
  - Access after 1-day Workshop
- IPAM Admins (Core Team)
  - Full DNS and DHCP Access
  - Access after certified Participation in Vendor Training
- External Resources
  - Classified based on Experience and Requirements
  - Assigned to one of the above Roles

External Authentication

- External Authentication doesn't replace in-database User Management
- External Authentication Systems often DNS-dependent
- IPAM Admins should not rely solely on external Services
- Allow Core Network Management even if Authentication System fails

Revocation of granted Access

- IPAM Users and Operators
  - Access via Group Membership in external Authentication System
  - Adjust Account if Department Changes or User leaves the Company
- IPAM Administrators
  - Regular Access like other Users via external Authentication System
  - Emergency Accounts need immediate Action (update, revoke, delete)

Password Life Cycle

- Centralized Management of Credentials in official Password Vault
- Password Vault used for complex Passwords Creation
- Enforcement of proper Password Complexity in IPAM Systems
- Implementation of Password Rotation (quarterly/semi-annual/annual)
- Automated Backup of Password Vault to safe Place

Patch and Update Management

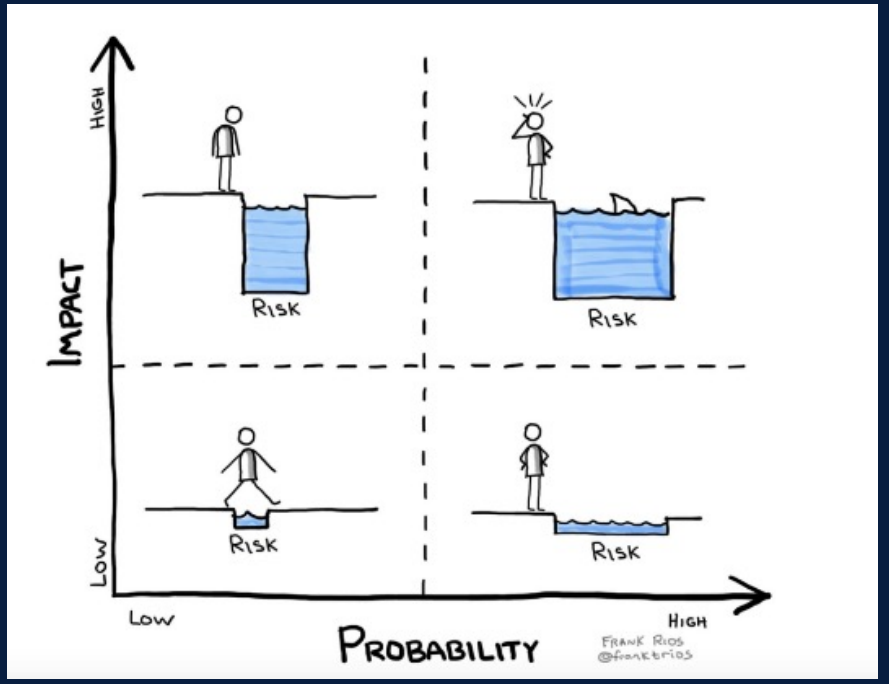
Types of Software Releases

- Major — significant Changes and Improvements from previous Major Version
- Minor — non-severe Changes and Improvements from previous Minor Version
- Maintenance — only applies to the current Releases (Major or Minor)
- Hotfix — addresses current and critical Problem in the Product

Patch and Update Management

Criticality of Software Releases

- Criticality of Vulnerability
- Probability of Occurrence of Attack or Problem
- Protection Needs of affected Data



Patch and Update Management

Software Update Implementation Procedure

1) Review, Communication, Download and Evaluation
2) Consolidation of environmental Tests
3) Test Results (feasibility, anomalies, time and effort)
4) Health Check before Installation
5) Productive Environment Update Plan
6) Maintenance Announcements
7) Installation in productive Environment
8) Monitoring and Conclusion

Lab and Consolidation Environment

Lab Environment

- Verify architectural Changes
- Test Software Upgrades with real-world Data
- Minimal Setup to validate Interoperability
- No Exchange with productive Environment

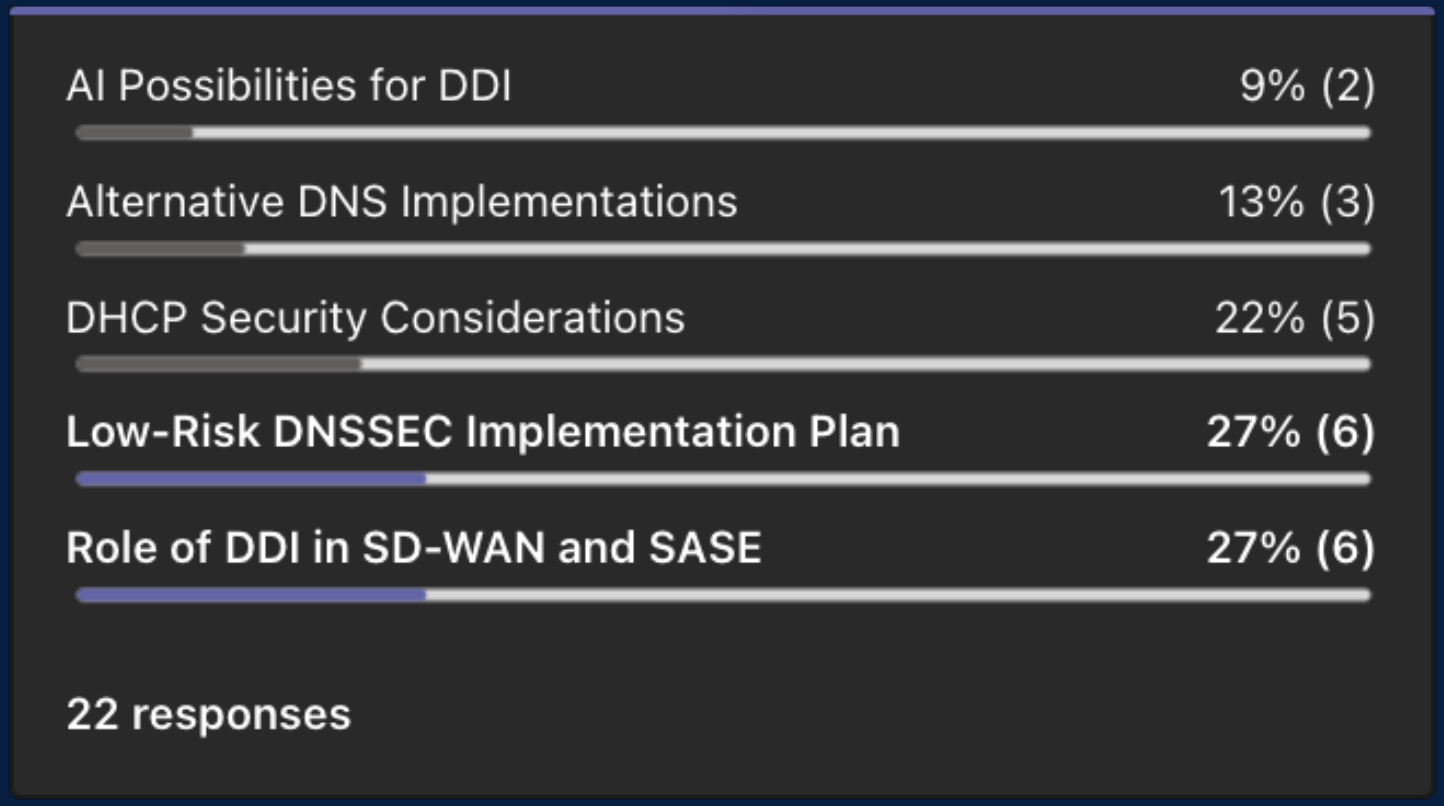
Consolidation Environment

- Tests new Features, Software and Hardware
- Tests Configurations and Use-Cases
  - DHCP Failover, Anycast DNS, 3rd-Parties, etc.

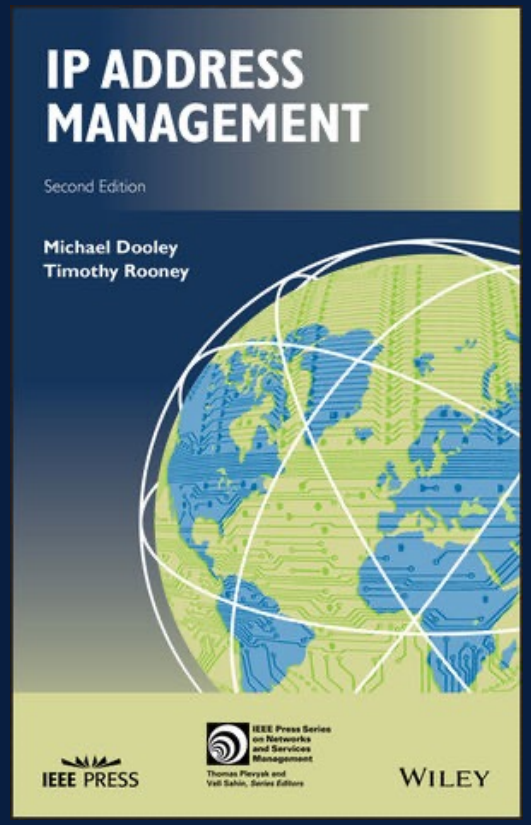
Frequent Inspection

- Health Checks — regularly by Core Team (monthly/quarterly)
- Security Reviews — regularly by Security Department incl. the Core Team (quarterly/semi-annually)
- Architecture Reviews — annually by Core Team (best practices, DNS/DHCP legacies, authorization concept)

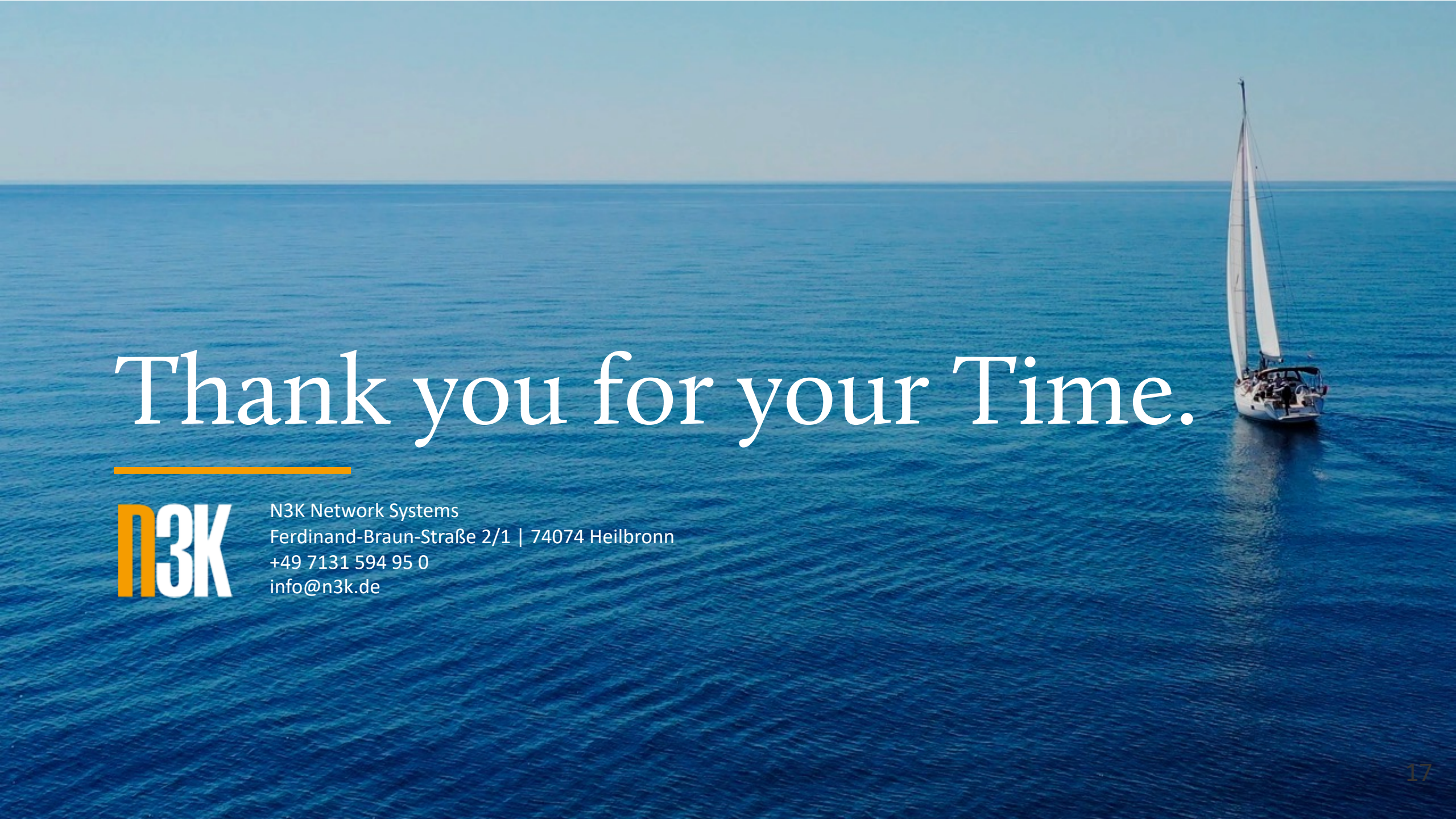
What's next?


AI Possibilities for DDI
9% (2)
Alternative DNS Implementations
13% (3)
DHCP Security Considerations
22% (5)
Low-Risk DNSSEC Implementation Plan
27% (6)
Role of DDI in SD-WAN and SASE
27% (6)
22 responses

Greedy for more?



https://www.wiley.com/en-us/IP+Address+Management,+2nd+Edition-p-9781119692270



Thank you for your Time.

N3K Network Systems
Ferdinand-Braun-Straße 2/1 | 74074 Heilbronn
+49 7131 594 95 0
info@n3k.de