Inclusive Security Guidelines for Authentication and Account Recovery

An Inclusive Threat Modelling Approach for Users with Multiple Sclerosis (MS)

Snow White

Produced as part of an Honours Project

BSc (Hons) Ethical Hacking

2026

Note that Information contained in this document is for educational purposes.

.

Executive Summary

Authentication and account recovery processes are crucial elements of a cybersecurity system; however, they are often associated with cognitive, physical, and usability demands that can have a higher impact on people with a disability. Individuals with MS can present with a lack of energy, cognitive cloudiness, memory difficulty, and motor or sensory problems that can increase a high risk of errors, lockouts and unhealthy coping behaviours.

These Inclusive Security Guidelines have been developed in accordance with the results of the combined STRIDE security and LINDDUN privacy threat modelling approach, which itself formed the basis of the adapted version of this approach with specific focus placed on the concept of accessibility.

These guidelines have been developed to be of use to designers, developers, and security professionals who wish to effectively implement inclusivity and make their security measures accessible to users without weakening their security features.

.

1 TABLE OF CONTENTS

2 Introduction 1

2.1 Purpose of the Guidelines 1

2.2 Intended Audience 1

2.3 Scope 1

3 Methodological Basis 2

4 Guideline Overview 3

Inclusive Security Guidelines 4

4.1 Guideline 1: Reduce Cognitive Load in Authentication and Recovery 4

4.2 Guideline 2: Provide Accessible Authentication Choices 4

4.3 Guideline 3: Design Account Recovery to Avoid Lockout Spirals 5

4.4 Guideline 4: Ensure Privacy and Transparency Throughout Security Flows 6

5 Standards Alignment 7

6 Limitations 8

7 Conclusions 9

.

2 INTRODUCTION

2.1 PURPOSE OF THE GUIDELINES

The purpose of this document is to offer practical and evidence-informed information on the design of authentications/user recovery that accommodates users with Multiple Sclerosis. These guidelines do not view accessibility as a secondary consideration to other aspects of usability. Instead, they view the barriers to accessibility as a place where security and privacy risk can exist.

These guidelines translate the results obtained out of an inclusive threat modelling process with STRIDE and LINDDUN into actionable design advice with decreased cognitive load, error recovery capabilities, and limited privacy exposure for critical security-related activities.

2.2 INTENDED AUDIENCE

These guidelines are intended for:

- Cybersecurity practitioners and threat modellers
- UX and interaction designers working on authentication systems
- Web developers implementing login and recovery flows
- Accessibility advocates and organisations supporting disabled users
- Healthcare or third-sector stakeholders evaluating digital inclusion

2.3 SCOPE

These guidelines apply to user-facing security processes in the following areas:

- User registration and credential creation
- Login and Authentication
- Account recovery and password reset

These systems do not try to replace backend security engineering practices; instead, they complement them by dealing with those risks that exist between security, usability, and accessibility.

3 METHODOLOGICAL BASIS

These guidelines are based upon:

- **STRIDE threat modelling**, identifying security threats such as spoofing, denial of service, and information disclosure
- **LINDDUN privacy analysis**, identifying risks such as detectability, unawareness, and linkability
- **WCAG 2.2 Accessible Authentication** success criteria (3.3.8 and 3.3.9)
- Qualitative accessibility research on MS-related impairments

The threats were prioritized if inaccessibility increased potential risk for security or privacy, such as susceptibility to increased levels of phishing, account lockout spirals, or insecure credential use.

4 GUIDELINE OVERVIEW

Guideline	Primary Focus	STRIDE Categories	LINDDUN Categories	MS-Related Impact
G1	Cognitive load reduction	DoS, Spoofing	Unawareness	Fatigue, cognitive fog
G2	Accessible authentication choices	Spoofing, Elevation of Privilege	Identifiability	Memory, motor impairment
G3	Inclusive account recovery	DoS, Tampering	Detecability	Error recovery difficulty
G4	Privacy and transparency	Information Disclosure	Detectability, Unawareness	Anxiety, trust

INCLUSIVE SECURITY GUIDELINES

4.1 GUIDELINE 1: REDUCE COGNITIVE LOAD IN AUTHENTICATION AND RECOVERY

Intent

Authentication mechanisms should require minimal cognitive processing on the users' parts, with the objective of avoiding human error, fatigue, or apathy. For users with MS, cognitive fog or diminished cognitive processing speed can severely hinder their interaction with time-intensive security measures.

Threats Addressed

- **STRIDE:** Denial of Service, Spoofing
- **LINDDUN:** Unawareness, Detectability

Design Recommendations

- Use plain language and concise instructions
- Avoid jargon and security-specific terminology where possible
- Eliminate memory-dependent tasks (e.g., recalling hints or codes)
- Avoid unnecessary time pressure or countdowns
- Allow safe retry without escalating penalties

Rationale

High cognitive load increases the probability of authentication failures, resulting in end users being unable to log on or growing frustrated. These states increase the risk of falling victim to phishing attacks or behaviors such as creating weak passwords and sharing these passwords with others. Decreasing cognitive load directly addresses the problem for usability and security.

4.2 GUIDELINE 2: PROVIDE ACCESSIBLE AUTHENTICATION CHOICES

Intent

Authentication mechanisms should support physical, cognitive, or sensory differences through the implementation of multiple transcription-free mechanisms instead of precision-based input devices.

Threats Addressed

- **STRIDE:** Spoofing, Elevation of Privilege
- **LINDDUN:** Identifiability

Design Recommendations

- Prefer phishing-resistant authentication methods where feasible

- Avoid long numeric codes or manual transcription
- Support device-based approvals or passwordless mechanisms
- Ensure compatibility with assistive technologies
- Maintain clear focus order and keyboard accessibility

Rationale

Authentication methods, like input requirements or memory recall of information, place disproportionate difficulties on people living with MS." These difficulties have the potential to lead to high rates of errors by the users, causing the individuals to skip various security measures. Making authentication more accessible reduces attack surfaces by promoting safe usage behaviors.

4.3 GUIDELINE 3: DESIGN ACCOUNT RECOVERY TO AVOID LOCKOUT SPIRALS

Intent

Account recovery mechanisms must support the user through failure without escalating repeated lockouts or exclusion.

Threats Addressed

- **STRIDE:** Denial of Service, Tampering
- **LINDDUN:** Detectability

Design Recommendations

- Provide multiple recovery paths (e.g., email and device approval)
- Avoid CAPTCHA-only recovery flows
- Use consistent and supportive error messages
- Implement adaptive rate-limiting rather than hard lockouts

Rationale

Account recovery is a highly vulnerable stage for both security and accessibility, repeated failures block legitimate access and raise the likelihood of social engineering or other abuses in recovery processes. Inclusive recovery design diminishes risks of service denial while supporting user autonomy.

4.4 GUIDELINE 4: ENSURE PRIVACY AND TRANSPARENCY THROUGHOUT SECURITY FLOWS

Intent

Authentication mechanisms should convey their actions without exposing information or permitting account enumeration.

Threats Addressed

- **STRIDE:** Information Disclosure
- **LINDDUN:** Detectability, Unawareness

Design Recommendations

- Use uniform system responses regardless of account existence
- Avoid revealing personal data in alerts or error messages
- Explain next steps clearly during recovery
- Minimize data displayed during authentication events

Rationale

Too little transparency can lead to confusion and user anxiety, whereas too much feedback can compromise user privacy. The level of feedback must be consistent to maintain privacy while promoting user trust and cognitive understanding.

5 STANDARDS ALIGNMENT

These guidelines align with the following standards:

- **WCAG 2.2** – Accessible Authentication (SC 3.3.8, 3.3.9)
- **NIST SP 800-63** – Digital Identity Guidelines
- **FIDO Alliance UX and Accessibility Guidance**

Alignment demonstrates compatibility with established best practice without claiming formal compliance.

6 LIMITATIONS

These guidelines are informed by qualitative threat modelling and are not an alternative to security audits and/or compliance standards. They are derived from the interface rather than the backend systems and are system specific.

7 CONCLUSIONS

These guidelines in Inclusive Security highlight this by directly considering accessibility issues in threat These Inclusive Security Guidelines will integrate accessibility considerations directly into threat modelling to show how security and usability goals can be mutually reinforced. Meeting the needs of users with MS will not only improve accessibility but also reduce security and privacy risks that affect all users. These guidelines provide a practical foundation for more inclusive and resilient authentication systems.