**Descrizione del Protocollo MPS[[1]](#footnote-2) tramite logica BAN**

**Protocollo Reale Autenticazione**

: A → S: ||

: S → A: ||

: A → S: ||

**Protocollo Idealizzato Autenticazione**

: A → S: ||

: S → A: ||

: A → S: ||

**Analisi Autenticazione**

**Obiettivi**

, # Session ID Establishing

**Assunzioni**

# Server Key Registration

# Key Registration

# Nonce Authority

# Freshness

Dopo :

Dopo :

Dopo :

**Protocollo Reale Scambio Chiavi Online**

: A → S: ||

: S → A: ||

: A → B: ||

: B → A: ||

: A → B:

: A → B:

**Protocollo Idealizzato Scambio Chiavi Online**

: A → S: ||

: S → A: ||

: A → B: ||

: B → A: ||

: A → B:

**Analisi Scambio Chiavi Online**

**Obiettivi**

, # Key Authentication

, # Key Confirmation

**Assunzioni**

, # Server Key Registration

, # Key Registration

, , # Freshness of the nonce used during the authentication protocol

# Jurisdiction Rule

# Authority on Y parameters

Dopo :

Dopo :

Dopo :

\*MPS postulated (verify)

Dopo :

Dopo :

**Protocollo Reale Scambio Chiavi Offline**

: A → S: ||

: S → A: ||

: A → S: ||

**Protocollo Idealizzato Scambio Chiavi Offline**

: A → S: ||

: S → A: ||

**Analisi Scambio Chiavi Online**

**Obiettivi**

# Get B’s Public Key

**Assunzioni**

, # Server Key Registration

, # Key Registration

, # Freshness of the nonce used during the authentication protocol

Dopo :

Dopo :

1. Magherini – Pochiero – Sieni (MPS) [↑](#footnote-ref-2)