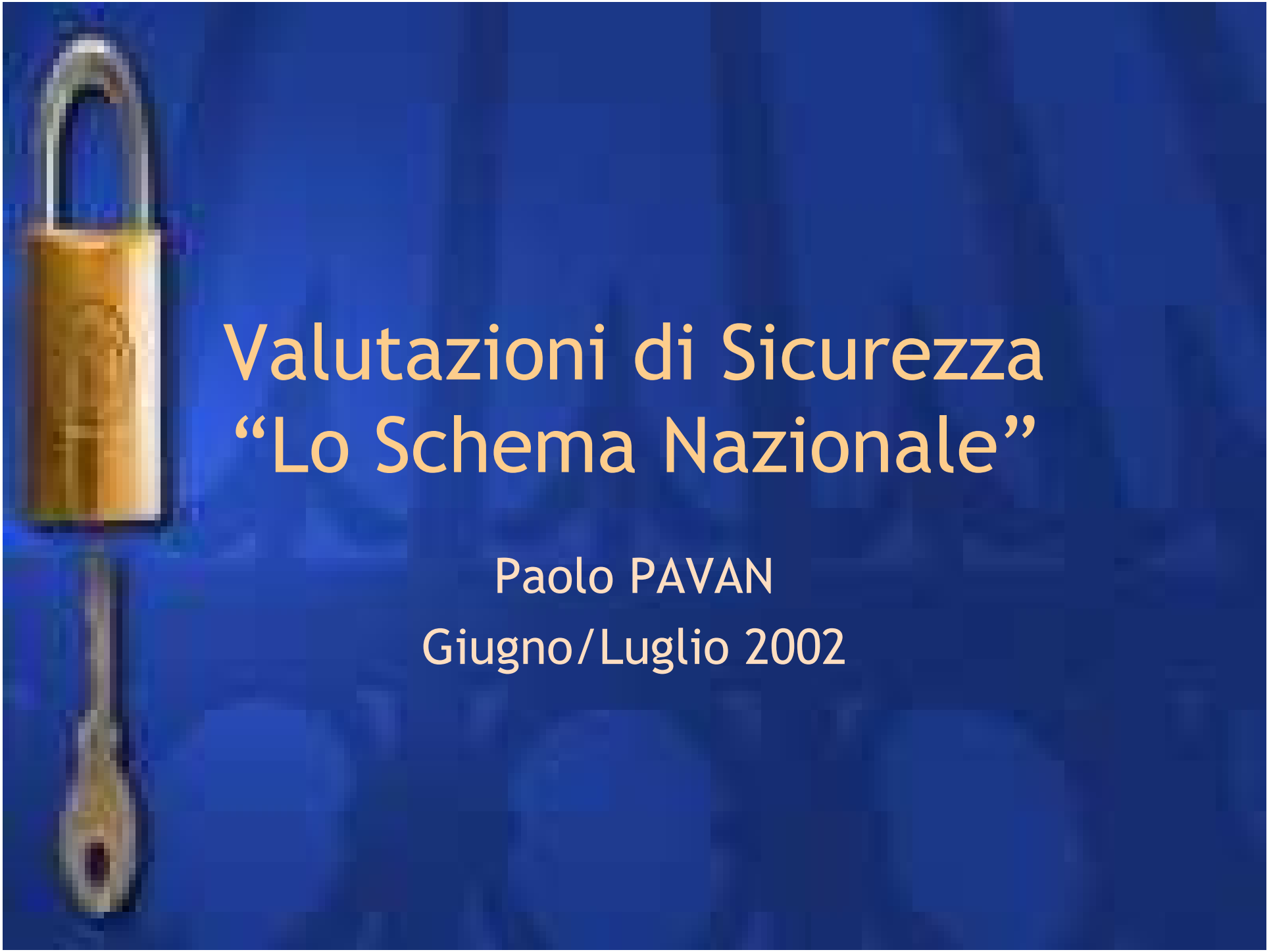
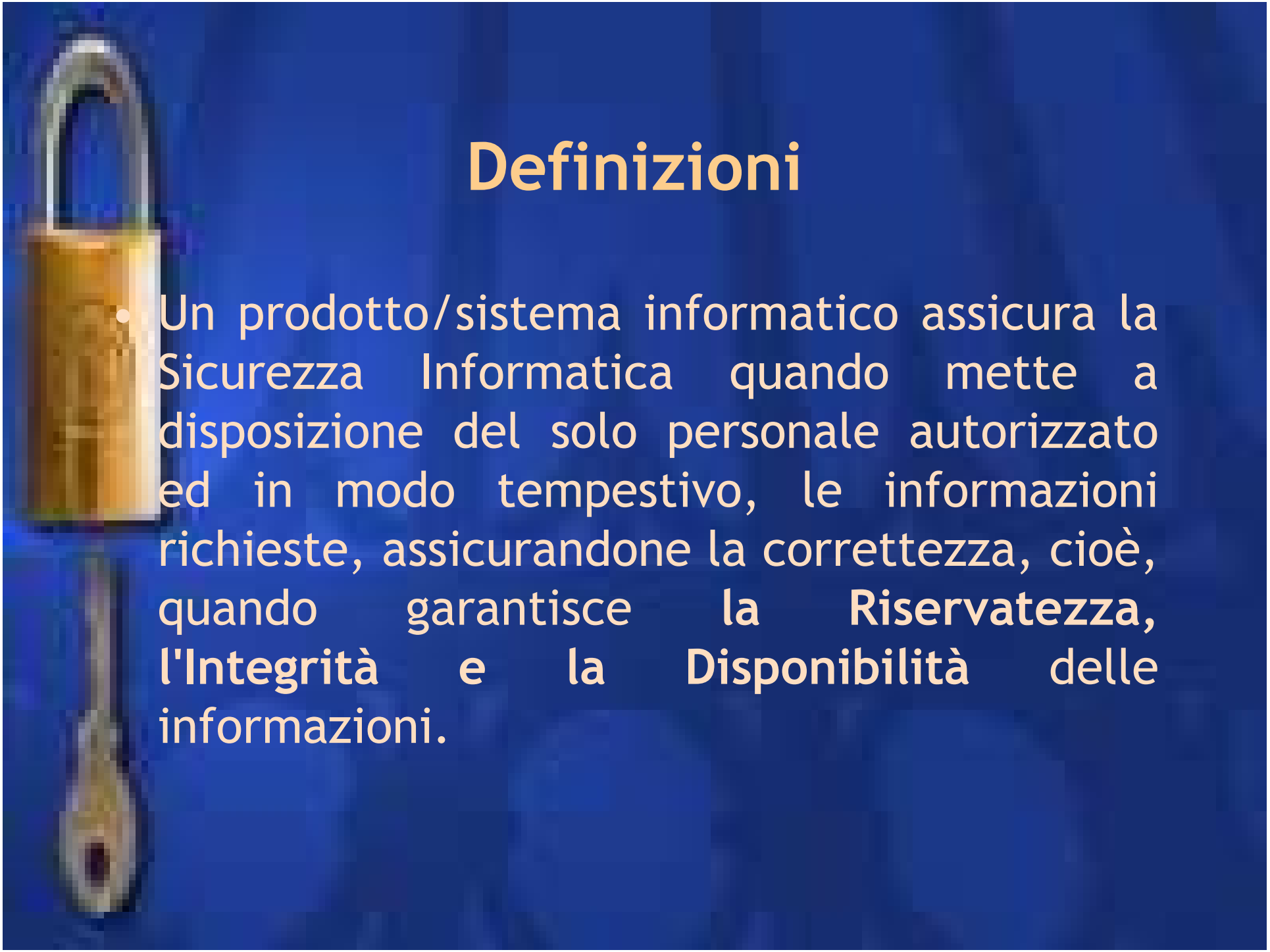


Valutazioni di Sicurezza “Lo Schema Nazionale”

Paolo PAVAN

Giugno/Luglio 2002



Definizioni

- Un prodotto/sistema informatico assicura la Sicurezza Informatica quando mette a disposizione del solo personale autorizzato ed in modo tempestivo, le informazioni richieste, assicurandone la correttezza, cioè, quando garantisce **la Riservatezza, l'Integrità e la Disponibilità** delle informazioni.

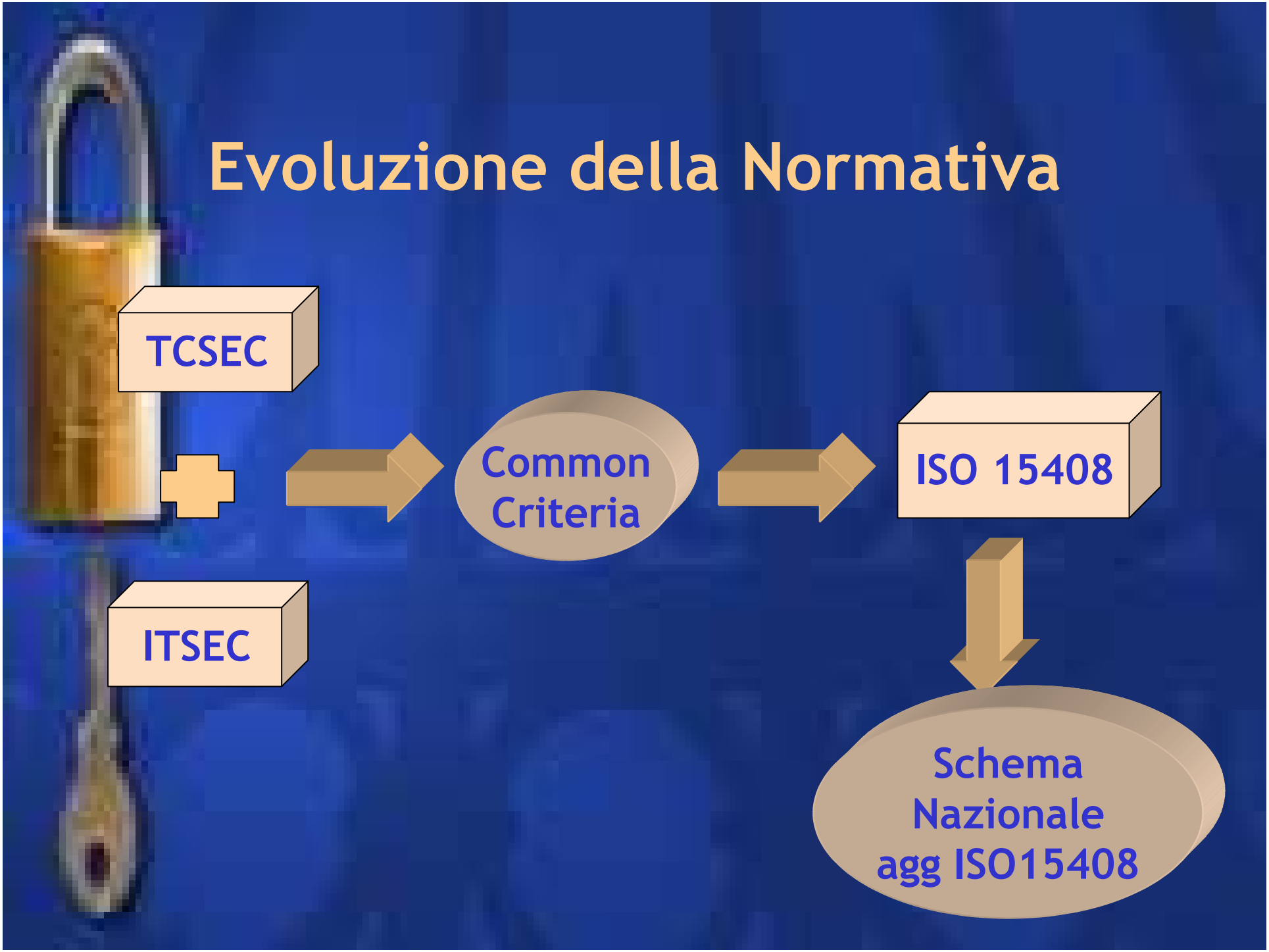
Perché richiedere una Valutazione

- L'utilizzatore di un particolare prodotto/sistema può richiedere che gli venga data una garanzia (assurance) che le funzionalità concepite per il raggiungimento della Sicurezza Informatica richiesta siano concettualmente efficaci e correttamente realizzate, cioè che il rischio residuo associato all'uso del sistema/prodotto sia effettivamente quello **definito come accettabile**.

Deve pertanto essere svolta un'attività di verifica (Valutazione) su tutti le fasi dello sviluppo, realizzazione e gestione del prodotto/sistema aventi un impatto sulla Sicurezza Informatica .

- La **Valutazione va effettuata da un organismo indipendente** che deve essere inserito in un meccanismo che assicuri la qualità del lavoro eseguito.

Evoluzione della Normativa



Gli Attori del Processo di Valutazione

- **L'Organizzazione Richiedente**: è dell'utilizzatore finale del prodotto/sistema che provvede a specificare le caratteristiche tecniche, operative ed in particolare di sicurezza richieste.
- **Il Fornitore**: l'organizzazione che si assume la responsabilità di fornire un prodotto/sistema che soddisfi alle specifiche tecniche, operative e di sicurezza richieste.
- **Il Centro di Valutazione - Ce.Va.**: **l'organizzazione indipendente** che incaricata dello Sponsor esegue la valutazione, **rispondendo esclusivamente all'Ente Certificatore** ed applicando criteri e metodologie dello Schema Nazionale: lo Sponsor è l'organizzazione che sostiene i costi della valutazione: può essere il fornitore o l'organizzazione richiedente.
  - Esempio in Italia: http://www.consorzio-res.it/
- **L'Ente Certificatore**: l'organizzazione che sorvegliando l'operato del Ce.Va. ed approvandone i risultati certifica il livello di garanzia del prodotto/sistema, è garante dell'applicazione dei criteri e metodologie previsti dallo **Schema Nazionale** per la valutazione. In generale l'Ente Certificatore è **l'Autorità Nazionale per la Sicurezza** o un'emanazione di essa che in Italia è conosciuta come **l'A.N.S.**

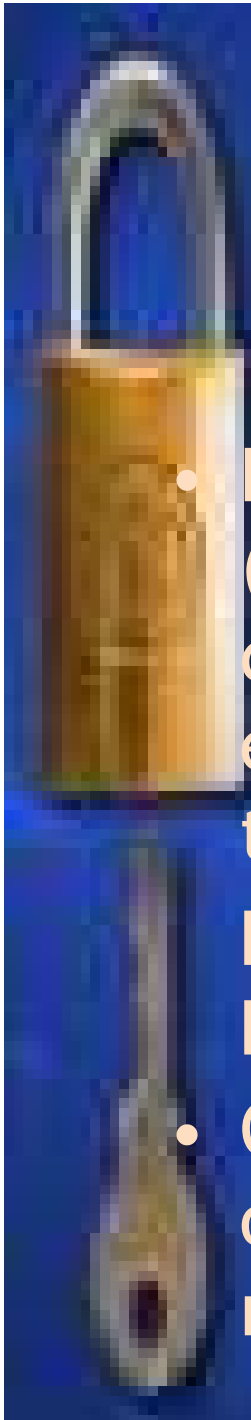
Svolgimento della Valutazione

- Consiste nell'analisi della documentazione che il Fornitore deve mettere a disposizione del Ce.Va. secondo modalità e livelli di dettaglio e formalismo dettati dallo Schema Nazionale.
- Il documento principale, che e anche il primo ad essere esaminato, è il **Security Target** nel quale lo sponsor, oltre a descrivere le funzioni dell'Oggetto della Valutazione **(ODV),** dichiara quali sono le politiche di sicurezza adottate, le misure procedurali, le funzioni ed i meccanismi impiegati per fronteggiare le minacce, il grado di robustezza dei meccanismi ed il livello di valutazione richiesto.
- Il Ce.Va. durante la Valutazione deve verificare:
  - l'Efficacia delle contromisure concepite per contrastare le minacce definite nel Security Target nel corso del normale uso del prodotto/sistema;
  - la Correttezza della realizzazione delle funzioni di sicurezza.
- Inoltre effettua anche ispezioni per verificare che il contenuto dei documenti ricevuti corrisponda alla realtà ed esegue test di penetrazione sull'oggetto della valutazione.

Livelli di Valutazione

- Non esiste un metodo univoco per la scelta del livello di valutazione.
- Quello proposto per reti EAD militari si basa sui seguenti criteri:
  - Livello tecnico dell'aggressore
  - Grado di esposizione del sistema
  - Appetibilità dei dati
  - Livello di classifica dei dati
  - Modalità operativa del sistema
  - Numero utenti
  - Quantità di dati
  - Vulnerabilità iniziale
  - Contromisure adottate

Campo di applicazione dello Schema Nazionale



- L'Ente Certificatore italiano, cioè l'**A.N.S.** (Autorità Nazionale per la Sicurezza), per disposizione di legge si deve occupare esclusivamente di tutto ciò che riguarda la tutela del segreto di Stato e pertanto non può occuparsi di valutazioni di prodotti/sistemi di uso diverso;
- Questa è una grave mancanza nel nostro ordinamento che dovrà essere la più presto risolta.

Se uno sponsor richiede una Valutazione?

- Ad oggi se uno Sponsor richiede una valutazione di un prodotto/sistema non destinato a trattare dati coperti dal segreto di Stato, l'A.N.S. non può esercitare la sua azione di garante e Certificatore
- in questo caso viene eseguita una valutazione "Conforme" alle norme ITSEC e ITSEM, cioè il Ce.Va. rilascia un "Certificato di Conformità" alle norme ITSEC (Common Criteria)

Campi di Applicazioni Internazionali

- I paesi che hanno svilupatto ITSEC e ITSEM cioè Gran Bretagna, Olanda, Francia e Germania riconoscono tra loro i prodotti certificati secondo la normativa comune (mutuamente).
- Questo vale solo per prodotti che non hanno a che fare con il Segreto di distato o la Difesa Nazionale in quel caso è stato costituito il SOG-IS ente formato dai medesimi paesi che verifica l'aderenza a standard di qualità applicati per tutti i paesi aderenti (non mutuamente).