Credential Networks: a General Model for Distributed Trust and Authenticity Management

Jacek Jonczy & Rolf Haenni

Reasoning under UNcertainty Group
Institute of Computer Science and Applied Mathematics
University of Berne, Switzerland

PST’05

October 12-14, 2005
Outline

1. Introduction
2. Credential Networks
3. Evaluation
4. Conclusion
Outline

1. Introduction
2. Credential Networks
3. Evaluation
4. Conclusion
Outline

1. Introduction
2. Credential Networks
3. Evaluation
4. Conclusion
Outline

1. Introduction
2. Credential Networks
3. Evaluation
4. Conclusion
Authenticity and Trust

World 1: (Public Key) Cryptography
- PKI
- Certificates ➝ Authenticity
- Question: Is the certifying entity trustworthy?

World 2: E-Business
- Reputation Network
- Ratings/Recommendations (digitally signed) ➝ Trust
- Question: Is an entity's public key authentic?
Authenticity and Trust

World 1: (Public Key) Cryptography
- PKI
- Certificates ➝ Authenticity
- Question: Is the certifying entity trustworthy?

World 2: E-Business
- Reputation Network
- Ratings/Recommendations (digitally signed) ➝ Trust
- Question: Is an entity's public key authentic?
Authenticity and Trust

World 1: (Public Key) Cryptography
- PKI
- Certificates ➝ Authenticity
- Question: Is the certifying entity trustworthy?

World 2: E-Business
- Reputation Network
- Ratings/Recommendations (digitally signed) ➝ Trust
- Question: Is an entity's public key authentic?
Introduction

Credential Networks

Evaluation

Conclusion

Authenticity and Trust

World 1: (Public Key) Cryptography
- PKI
- Certificates → **Authenticity**
- Question: Is the certifying entity trustworthy?

World 2: E-Business
- Reputation Network
- Ratings/Recommendations (digitally signed) → **Trust**
- Question: Is an entity's public key authentic?
Authenticity and Trust

World 1: (Public Key) Cryptography
- PKI
- Certificates $\rightarrow$ **Authenticity**
  - Question: Is the certifying entity trustworthy?

World 2: E-Business
- Reputation Network
- Ratings/Recommendations (digitally signed) $\rightarrow$ **Trust**
  - Question: Is an entity's public key authentic?

Two-Layer Model
Outline

1. Introduction
2. Credential Networks
3. Evaluation
4. Conclusion
Example

C1 A: "I am quite sure (80%) that B’s public key is authentic."

C2 A: "I assume (50%) that C’s public key is authentic."

C3 B: "I believe (60%) in the authenticity of C’s public key."

C4 B: "I have some doubts (30%) that D’s public key is authentic."

C5 C: "On a scale between 0 and 1, I would rate the authenticity of D’s public key with 0.9."

C6 A: "I am almost sure (90%) that B is trustworthy."

C7 A: "I believe (70%) in C’s trustworthiness."

C8 B: "On a scale between 0 and 1, I would rate D’s trustworthiness with 0.4."
Example

C1  A: "I am quite sure (80%) that B’s public key is authentic."

C2  A: "I assume (50%) that C’s public key is authentic."

C3  B: "I believe (60%) in the authenticity of C’s public key."

C4  B: "I have some doubts (30%) that D’s public key is authentic."

C5  C: "On a scale between 0 and 1, I would rate the authenticity of D’s public key with 0.9."

C6  A: "I am almost sure (90%) that B is trustworthy."

C7  A: "I believe (70%) in C’s trustworthiness."

C8  B: "On a scale between 0 and 1, I would rate D’s trustworthiness with 0.4."
Example

C1: "I am quite sure (80%) that B’s public key is authentic.”

C2: "I assume (50%) that C’s public key is authentic.”

C3: "I believe (60%) in the authenticity of C's public key.”

C4: "I have some doubts (30%) that D’s public key is authentic.”

C5: "On a scale between 0 and 1, I would rate the authenticity of D’s public key with 0.9.”

C6: "I am almost sure (90%) that B is trustworthy.”

C7: "I believe (70%) in C’s trustworthiness.”

C8: "On a scale between 0 and 1, I would rate D’s trustworthiness with 0.4.”
Example

C1: "I am quite sure (80%) that B’s public key is authentic."

C2: "I assume (50%) that C’s public key is authentic."

C3: "I believe (60%) in the authenticity of C’s public key."

C4: "I have some doubts (30%) that D’s public key is authentic."

C5: "On a scale between 0 and 1, I would rate the authenticity of D’s public key with 0.9."

C6: "I am almost sure (90%) that B is trustworthy."

C7: "I believe (70%) in C’s trustworthiness."

C8: "On a scale between 0 and 1, I would rate D’s trustworthiness with 0.4."
Example

C1: "I am quite sure (80%) that B’s public key is authentic."

C2: "I assume (50%) that C’s public key is authentic."

C3: "I believe (60%) in the authenticity of C’s public key."

C4: "I have some doubts (30%) that D’s public key is authentic."

C5: "On a scale between 0 and 1, I would rate the authenticity of D’s public key with 0.9."

C6: "I am almost sure (90%) that B is trustworthy."

C7: "I believe (70%) in C’s trustworthiness."

C8: "On a scale between 0 and 1, I would rate D’s trustworthiness with 0.4."
Example

C1: "I am quite sure (80%) that B’s public key is authentic.”

C2: "I assume (50%) that C’s public key is authentic.”

C3: "I believe (60%) in the authenticity of C's public key.”

C4: "I have some doubts (30%) that D’s public key is authentic.”

C5: "On a scale between 0 and 1, I would rate the authenticity of D’s public key with 0.9.”

C6: "I am almost sure (90%) that B is trustworthy.”

C7: "I believe (70%) in C’s trustworthiness.”

C8: "On a scale between 0 and 1, I would rate D’s trustworthiness with 0.4.”
Example

C1: "I am quite sure (80%) that B’s public key is authentic."

C2: "I assume (50%) that C’s public key is authentic."

C3: "I believe (60%) in the authenticity of C’s public key."

C4: "I have some doubts (30%) that D’s public key is authentic."

C5: "On a scale between 0 and 1, I would rate the authenticity of D’s public key with 0.9."

C6: "I am almost sure (90%) that B is trustworthy."

C7: "I believe (70%) in C’s trustworthiness."

C8: "On a scale between 0 and 1, I would rate D’s trustworthiness with 0.4."
Example

C1 A: "I am quite sure (80%) that B’s public key is authentic.”

C2 A: "I assume (50%) that C’s public key is authentic.”

C3 B: "I believe (60%) in the authenticity of C’s public key.”

C4 B: "I have some doubts (30%) that D’s public key is authentic.”

C5 C: "On a scale between 0 and 1, I would rate the authenticity of D’s public key with 0.9.”

C6 A: "I am almost sure (90%) that B is trustworthy.”

C7 A: "I believe (70%) in C’s trustworthiness.”

C8 B: "On a scale between 0 and 1, I would rate D’s trustworthiness with 0.4.”
Example

C1: "I am quite sure (80%) that B’s public key is authentic."

C2: "I assume (50%) that C’s public key is authentic."

C3: "I believe (60%) in the authenticity of C’s public key."

C4: "I have some doubts (30%) that D’s public key is authentic."

C5: "On a scale between 0 and 1, I would rate the authenticity of D’s public key with 0.9."

C6: "I am almost sure (90%) that B is trustworthy."

C7: "I believe (70%) in C’s trustworthiness."

C8: "On a scale between 0 and 1, I would rate D’s trustworthiness with 0.4."
Credentials

- A **credential** is a digitally signed statement concerning a user’s \(X\) authenticity (\(Aut_X\)) or trustworthiness (\(Trust_X\)).
- Credential \(C = (\text{class}, \text{sign}, \text{issuer}, \text{recipient}, \text{weight})\)

\[
\begin{align*}
\text{class} &\in \{T,A\}, \\
\text{sign} &\in \{+, -, \pm\}, \\
\text{issuer}, \text{recipient} &\in \mathcal{U}_0, \\
\text{weight} &\in [0,1].
\end{align*}
\]

- Six possible credential types: \(\{T, A\} \times \{+, -, \pm\}\)
- **A-credentials:**

\[
A_{\text{issuer}, \text{recipient}}^{\text{sign}, \text{weight}} = (A, \text{sign}, \text{issuer}, \text{recipient}, \text{weight})
\]

- **T-credentials:**

\[
T_{\text{issuer}, \text{recipient}}^{\text{sign}, \text{weight}} = (T, \text{sign}, \text{issuer}, \text{recipient}, \text{weight})
\]
Credential Networks: The Model

Definition

A credential network is a tuple

\[ \mathcal{N} = (\mathcal{U}_0, \mathcal{X}_0, \mathcal{C}) \]

where

\( \mathcal{U}_0 \) = set of all users \( X_0, X_1, X_2, \ldots, X_n \)

\( \mathcal{X}_0 \) = owner of the network

\( \mathcal{C} \) = set of credentials \( C_1, C_2, \ldots, C_m \)
Example

\[ \mathcal{U}_0 = \{A, B, C, D\} \]

\[ X_0 = A \]

\[ C = \left\{ A_{AB}^{+0.8}, A_{AC}^{+0.5}, A_{BC}^{+0.6}, T_{AB}^{+0.9}, T_{AC}^{+0.7}, A_{BD}^{-0.3}, A_{CD}^{\pm0.9}, T_{BC}^{\pm0.4} \right\} \]
Certificates & Recommendations

- **Type 1: Certificate**
  - is a positive A-credential $A_{XY}^{+\pi}$ issued by $X$ for $Y$
  - $Aut_X \land Trust_X \land A_{XY}^{+} \rightarrow Aut_Y$
  - $p(A_{XY}^{+}) = \pi$

- **Type 2: Recommendation**
  - is a positive T-credential $T_{XY}^{+\pi}$ issued by $X$ for $Y$
  - $Aut_X \land Trust_X \land T_{XY}^{+} \rightarrow Trust_Y$
  - $p(T_{XY}^{+}) = \pi$
Certificates & Recommendations

- **Type 1: Certificate**
  - is a positive A-credential $A_{XY}^+$ issued by $X$ for $Y$
  - $\text{Aut}_X \land \text{Trust}_X \land A_{XY}^+ \rightarrow \text{Aut}_Y$
  - $\pi(A_{XY}^+) = \pi$

- **Type 2: Recommendation**
  - is a positive T-credential $T_{XY}^+$ issued by $X$ for $Y$
  - $\text{Aut}_X \land \text{Trust}_X \land T_{XY}^+ \rightarrow \text{Trust}_Y$
  - $\pi(T_{XY}^+) = \pi$
Revocations & Discredits

- **Type 3: Revocation**
  - is a negative $A$-credential $A_{XY}^{-\pi}$ issued by $X$ for $Y$
  - $Aut_X \land Trust_X \land A_{XY}^{-\pi} \rightarrow \neg Aut_Y$
  - $p(A_{XY}^{-\pi}) = \pi$

- **Type 4: Discredit**
  - is a negative $T$-credential $T_{XY}^{-\pi}$ issued by $X$ for $Y$
  - $Aut_X \land Trust_X \land T_{XY}^{-\pi} \rightarrow \neg Trust_Y$
  - $p(T_{XY}^{-\pi}) = \pi$
Revocations & Discredits

- **Type 3: Revocation**
  - is a negative A-credential $A_{XY}^-\pi$ issued by $X$ for $Y$
  - $Aut_X \land Trust_X \land A_{XY}^- \rightarrow \neg Aut_Y$
  - $p(A_{XY}^-) = \pi$

- **Type 4: Discredit**
  - is a negative T-credential $T_{XY}^-\pi$ issued by $X$ for $Y$
  - $Aut_X \land Trust_X \land T_{XY}^- \rightarrow \neg Trust_Y$
  - $p(T_{XY}^-) = \pi$
Mixed Ratings

- **Type 5: Authenticity Rating**
  - is a mixed A-credential $A_{XY}^{\pm \pi}$ issued by $X$ for $Y$

$$Au_t_X \land Trust_X \land A_{XY}^{\pm \pi} \rightarrow Aut_Y,$$

$$Au_t_X \land Trust_X \land \neg A_{XY}^{\pm \pi} \rightarrow \neg Aut_Y.$$  

- $p(A_{XY}^{\pm \pi}) = \pi$, $p(\neg A_{XY}^{\pm \pi}) = 1 - \pi$

- **Type 6: Trust Rating**
  - is a mixed T-credential $T_{XY}^{\pm \pi}$ issued by $X$ for $Y$

$$Au_t_X \land Trust_X \land T_{XY}^{\pm \pi} \rightarrow Trust_Y,$$

$$Au_t_X \land Trust_X \land \neg T_{XY}^{\pm \pi} \rightarrow \neg Trust_Y.$$  

- $p(T_{XY}^{\pm \pi}) = \pi$, $p(\neg T_{XY}^{\pm \pi}) = 1 - \pi$
Mixed Ratings

- **Type 5: Authenticity Rating**
  - is a mixed A-credential $A_{XY}^{\pm \pi}$ issued by $X$ for $Y$
  
  $$Aut_X \land Trust_X \land A_{XY}^{\pm} \rightarrow Aut_Y,$$
  $$Aut_X \land Trust_X \land \neg A_{XY}^{\pm} \rightarrow \neg Aut_Y.$$

  $$p(A_{XY}^{\pm}) = \pi, \quad p(\neg A_{XY}^{\pm}) = 1 - \pi$$

- **Type 6: Trust Rating**
  - is a mixed T-credential $T_{XY}^{\pm \pi}$ issued by $X$ for $Y$
  
  $$Aut_X \land Trust_X \land T_{XY}^{\pm} \rightarrow Trust_Y,$$
  $$Aut_X \land Trust_X \land \neg T_{XY}^{\pm} \rightarrow \neg Trust_Y.$$

  $$p(T_{XY}^{\pm}) = \pi, \quad p(\neg T_{XY}^{\pm}) = 1 - \pi$$
Special Cases

Credential Networks include the following special cases:

- PGP’s Web of Trust
- Maurer’s Model
- Haenni’s Model
- Centralized Model (CA)
- Reputation Networks (in some sense)
- etc.

Similar models:

- Certificate Algebra (A. Jøsang)
- etc.
Outline

1. Introduction
2. Credential Networks
3. Evaluation
4. Conclusion
Evaluation: An Uncertain Reasoning Approach

Credential Network

\[ N = (U_0, X_0, C) \]

Probablistic Argumentation System (Kohlas, Haenni)

Hypothesis \( h \)

\( Aut_X \)

\( Trust_X \)

Knowledge Base \( \Sigma \)

Arguments

\( Args(h) \)

\( Args(\neg h) \)

Counter-Arguments

Degree of Support

\( dsp(h) \)

\( dsp(\neg h) \)
Evaluation: An Uncertain Reasoning Approach

Credential Network

\[ N = (U_0, X_0, C) \]

Probabilistic Argumentation System (Kohlas, Haenni)

\[ Aut_x \]

\[ Trust_x \]

Hypothesis \( h \)

Knowledge Base \( \sum \)

Arguments

\[ Args(h) \]

\[ Args(\neg h) \]

Counter-Arguments

Degree of Support

\[ dsp(h) \]

\[ dsp(\neg h) \]
Evaluation: An Uncertain Reasoning Approach

Credential Network

\[ N = (U_0, X_0, C) \]

Probablistic Argumentation System (Kohlas, Haenni)

Hypothesis \( h \)

\[ Aut_x \quad Trust_x \]

Knowledge Base \( \Sigma \)

Arguments

\[ Args(h) \quad Args(\neg h) \]

Counter-Arguments

Degree of Support

\[ dsp(h) \quad dsp(\neg h) \]
Evaluation: An Uncertain Reasoning Approach

Credential Network:

\[ N = (U_0, X_0, C) \]

Probabilistic Argumentation System (Kohlas, Haenni):

Hypothesis \( h \)

\[ Aut_X \]

\[ Trust_X \]

Knowledge Base \( \Sigma \)

1. Arguments

\[ Args(h) \]
\[ Args(\neg h) \]

Degree of Support

\[ dsp(h) \]
\[ dsp(\neg h) \]

Jacek Jonczy & Rolf Haenni
University of Berne, Switzerland
Evaluation: An Uncertain Reasoning Approach

Credential Network

\[ N = (U_0, X_0, C) \]

Probablistic Argumentation System

(Kohlas, Haenni)

Knowledge Base \( \Sigma \)

Arguments

\[ \text{Args}(h) \]
\[ \text{Args}(\neg h) \]

Counter-Arguments

\[ \text{dsp}(h) \]
\[ \text{dsp}(\neg h) \]

Degree of Support

1. \( Aut_X \)
2. \( Trust_X \)

Hypothesis \( h \)

Jacek Jonczy & Rolf Haenni
University of Berne, Switzerland
Evaluation: An Uncertain Reasoning Approach

Credential Network
\[ N = (U_0, X_0, C) \]

Probablistic Argumentation System (Kohlas, Haenni)

Knowledge Base \[ \Sigma \]

Hypothesis \( h \)

Aut\(_X^h\)  Trust\(_X^h\)

Arguments
\[ \text{Args}(h) \]
\[ \text{Args}(\neg h) \]

Counter-Arguments

Degree of Support
\[ 0 \leq \text{dsp}(h) + \text{dsp}(\neg h) \leq 1 \]
Probabilistic Argumentation System (PAS)

**Definition**

A PAS is a tuple

\[ \mathcal{S} = (V, W, \mathbf{P}, \Sigma) \]

such that

- \( V \) = set of propositional variables,
- \( \mathcal{L}_V \) = propositional language over \( V \),
- \( W \) = subset of \( V \) with \( \mathbf{P}(W) \),
- \( \Sigma \) = logical knowledge base \( \subseteq \mathcal{L}_V \).
Example

\[ W = \{ A_{AB}^+, A_{AC}^+, A_{CD}^\pm, T_{AB}^+, T_{AC}^+, A_{BC}^+, A_{BD}^-, T_{BD}^\pm \} \]

\[ V = W \cup \{ Aut_X, Trust_X : X \in \{ A, B, C, D \} \} \]

\[ \Sigma = \begin{cases} 
\text{Aut}_A \\
\text{Trust}_A \\
\text{Aut}_A \land \text{Trust}_A \land A_{AB}^+ \rightarrow \text{Aut}_B \\
\text{Aut}_A \land \text{Trust}_A \land A_{AC}^+ \rightarrow \text{Aut}_C \\
\text{Aut}_A \land \text{Trust}_A \land T_{AB}^+ \rightarrow \text{Trust}_B \\
\text{Aut}_A \land \text{Trust}_A \land T_{AC}^+ \rightarrow \text{Trust}_C \\
\text{Aut}_B \land \text{Trust}_B \land A_{BC}^+ \rightarrow \text{Aut}_C \\
\text{Aut}_B \land \text{Trust}_B \land T_{BD}^- \rightarrow \neg \text{Aut}_D \\
\text{Aut}_B \land \text{Trust}_B \land T_{BD}^\pm \rightarrow \text{Aut}_D \\
\text{Aut}_B \land \text{Trust}_B \land \neg T_{BD}^\pm \rightarrow \neg \text{Aut}_D \\
\text{Aut}_C \land \text{Trust}_C \land A_{CD}^\pm \rightarrow \text{Aut}_D \\
\text{Aut}_C \land \text{Trust}_C \land \neg A_{CD}^\pm \rightarrow \neg \text{Aut}_D 
\end{cases} \]

\[ P(W) : p(A_{AB}^+) = 0.8, \ p(T_{AB}^+) = 0.9, \ p(A_{BC}^+) = 0.6, \ldots \]
Qualitative Approach

**Arguments** for $\text{Aut}_X$, $\text{Trust}_X$, $\neg\text{Aut}_X$, $\neg\text{Trust}_X$:

\[
\text{args}(\text{Aut}_D) = \begin{cases} 
A^+_{AC} A^+_{CD} T^+_{AC}, \\
A^+_{AB} A^+_{AB} A^\pm_{CD} T^+_{AB} T^+_{AC} 
\end{cases}
\]

\[
\text{args}(\neg\text{Aut}_D) = \begin{cases} 
A^+_{AB} A^\pm_{AB} T^+_{AB}, \\
A^+_{AC} A^\pm_{CD} T^+_{AC}, \\
A^+_{AB} A^+_{AB} A^\pm_{CD} T^+_{AB} T^+_{AC} 
\end{cases}
\]

\[
\text{args}(\text{Trust}_D) = \begin{cases} 
A^+_{AB} T^+_{AB} T^\pm_{BD}, \\
A^+_{AB} A^+_{CD} A^\pm_{BD} T^+_{AB} T^+_{AC}, \\
A^+_{AB} A^+_{AB} A^-_{AC} A^\pm_{CD} T^+_{AB} T^+_{AC} 
\end{cases}
\]

\[
\text{args}(\neg\text{Trust}_D) = \begin{cases} 
A^+_{AB} T^+_{AB} T^\pm_{BD}, \\
A^+_{AB} A^+_{AB} A^-_{AC} A^\pm_{CD} T^+_{AB} T^+_{AC}, \\
A^+_{AB} A^+_{AB} A^-_{BD} A^\pm_{CD} T^+_{AB} T^+_{AC} 
\end{cases}
\]
Qualitative Approach

**Arguments** for $Aut_X$, $Trust_X$, $\neg Aut_X$, $\neg Trust_X$:

\[
\text{args}(Aut_D) = \left\{ \begin{array}{l}
A^+_{AC} A^{\pm}_{CD} T^+_{AC}, \\
A^+_{AB} A^+_{BC} A^{\pm}_{CD} T^+_{AB} T^+_{AC}
\end{array} \right. \\
\text{args}(\neg Aut_D) = \left\{ \begin{array}{l}
A^+_{AB} A^-_{BD} T^+_{AB}, \\
A^+_{AC} \neg A^{\pm}_{CD} T^+_{AC}, \\
A^+_{AB} A^+_{BC} \neg A^{\pm}_{CD} T^+_{AB} T^+_{AC}
\end{array} \right. \\
\text{args}(Trust_D) = \left\{ \begin{array}{l}
A^+_{AB} T^+_{AB} T^\pm_{BD}, \\
A^+_{AB} A^+_{BC} A^-_{BD} A^{\pm}_{CD} T^+_{AB} T^+_{AC}, \\
A^+_{AB} A^+_{AC} A^-_{BD} A^{\pm}_{CD} T^+_{AB} T^+_{AC}
\end{array} \right. \\
\text{args}(\neg Trust_D) = \left\{ \begin{array}{l}
A^+_{AB} T^+_{AB} \neg T^\pm_{BD}, \\
A^+_{AB} A^+_{BC} A^-_{BD} A^{\pm}_{CD} T^+_{AB} T^+_{AC}, \\
A^+_{AB} A^+_{AC} A^-_{BD} A^{\pm}_{CD} T^+_{AB} T^+_{AC}
\end{array} \right.
\]
Qualitative Approach

**Arguments** for $Aut_X$, $Trust_X$, $\neg Aut_X$, $\neg Trust_X$:

$$\text{args}(Aut_D) = \begin{cases} \{ A^+_A A^\pm_C T^+_A C D T^+_A C D \} \\ A^+_A B^+_A B C A^\pm_C D T^+_A B T^+_A C D \} \end{cases}$$

$$\text{args}(\neg Aut_D) = \begin{cases} \{ A^+_A B^+_A B D T^+_A B D \} \\ A^+_A A^\pm_C D T^+_A C D \} \\ A^+_A A^\pm_C D A^\pm_C D T^+_A B T^+_A C D \} \end{cases}$$

$$\text{args}(Trust_D) = \begin{cases} \{ A^+_A B^+_A B C A^\pm_C D T^+_A B T^+_A C D \} \\ A^+_A A^\pm_C D A^\pm_C D T^+_A B T^+_A C D \} \end{cases}$$

$$\text{args}(\neg Trust_D) = \begin{cases} \{ A^+_A B^+_A B D T^+_A B D \} \\ A^+_A A^\pm_C D A^\pm_C D T^+_A B T^+_A C D \} \end{cases}$$
Qualitative Approach

**Arguments** for $\text{Aut}_X$, $\text{Trust}_X$, $\neg\text{Aut}_X$, $\neg\text{Trust}_X$:

$$\text{args}(\text{Aut}_D) = \left\{ \begin{array}{c} A^+_{AC} A^\pm_{CD} T^+_{AC}, \\ A^+_{AB} A^+_{BC} A^\pm_{CD} T^+_{AB} T^+_{AC} \end{array} \right\}$$

$$\text{args}(\neg\text{Aut}_D) = \left\{ \begin{array}{c} A^+_{AB} A^-_{BD} T^+_{AB}, \\ A^+_{AC} A^-_{CD} T^+_{AC}, \\ A^+_{AB} A^+_{BC} A^-_{CD} T^+_{AB} T^+_{AC} \end{array} \right\}$$

$$\text{args}(\text{Trust}_D) = \left\{ \begin{array}{c} A^+_{AB} T^+_{AB} T^\pm_{BD}, \\ A^+_{AB} A^+_{BC} A^-_{BD} A^\pm_{CD} T^+_{AB} T^+_{AC}, \\ A^+_{AB} A^+_{AC} A^-_{BD} A^\pm_{CD} T^+_{AB} T^+_{AC} \end{array} \right\}$$

$$\text{args}(\neg\text{Trust}_D) = \left\{ \begin{array}{c} A^+_{AB} T^+_{AB} A^-T^\pm_{BD}, \\ A^+_{AB} A^+_{BC} A^-_{BD} A^\pm_{CD} T^+_{AB} T^+_{AC}, \\ A^+_{AB} A^+_{AC} A^-_{BD} A^\pm_{CD} T^+_{AB} T^+_{AC} \end{array} \right\}$$
Quantitative Approach

Computing degrees of support for $\text{Aut}_X$, $\text{Trust}_X$, $\neg\text{Aut}_X$, $\neg\text{Trust}_X$:

- Suppose threshold $\lambda = 0.7$ for accepting a hypotheses
  $\Rightarrow$ $\text{Aut}_A$, $\text{Trust}_A$, $\text{Aut}_B$ and $\text{Trust}_B$ accepted
- Suppose threshold $\eta = 0.4$ for rejecting a hypotheses
  $\Rightarrow$ $\text{Trust}_D$ rejected

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{dsp}(\text{Aut}_X)$</td>
<td>1</td>
<td>0.78</td>
<td>0.68</td>
<td>0.38</td>
</tr>
<tr>
<td>$\text{dsp}(\neg\text{Aut}_X)$</td>
<td>0</td>
<td>0.03</td>
<td>0.03</td>
<td>0.16</td>
</tr>
<tr>
<td>$\text{dsp}(\text{Trust}_X)$</td>
<td>1</td>
<td>0.89</td>
<td>0.66</td>
<td>0.27</td>
</tr>
<tr>
<td>$\text{dsp}(\neg\text{Trust}_X)$</td>
<td>0</td>
<td>0.01</td>
<td>0.05</td>
<td>0.41</td>
</tr>
</tbody>
</table>
Quantitative Approach

Computing **degrees of support** for $Aut_X, Trust_X, \neg Aut_X, \neg Trust_X$:

- Suppose threshold $\lambda = 0.7$ for *accepting* a hypotheses
  $\Rightarrow Aut_A, Trust_A, Aut_B$ and $Trust_B$ accepted
- Suppose threshold $\eta = 0.4$ for *rejecting* a hypotheses
  $\Rightarrow Trust_D$ rejected

<table>
<thead>
<tr>
<th></th>
<th>$A$</th>
<th>$B$</th>
<th>$C$</th>
<th>$D$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$dsp(Aut_X)$</td>
<td>1</td>
<td>0.78</td>
<td>0.68</td>
<td>0.38</td>
</tr>
<tr>
<td>$dsp(\neg Aut_X)$</td>
<td>0</td>
<td>0.03</td>
<td>0.03</td>
<td>0.16</td>
</tr>
<tr>
<td>$dsp(Trust_X)$</td>
<td>1</td>
<td>0.89</td>
<td>0.66</td>
<td>0.27</td>
</tr>
<tr>
<td>$dsp(\neg Trust_X)$</td>
<td>0</td>
<td>0.01</td>
<td>0.05</td>
<td>0.41</td>
</tr>
</tbody>
</table>
Quantitative Approach

Computing **degrees of support** for

\( Aut_X, Trust_X, \neg Aut_X, \neg Trust_X \):

- Suppose threshold \( \lambda = 0.7 \) for *accepting* a hypotheses
  \[ \Rightarrow Aut_A, Trust_A, Aut_B \text{ and } Trust_B \text{ accepted} \]
- Suppose threshold \( \eta = 0.4 \) for *rejecting* a hypotheses
  \[ \Rightarrow Trust_D \text{ rejected} \]

\[
\begin{array}{|c|c|c|c|}
\hline
 & A & B & C \\
\hline
dsp(Aut_X) & 1 & 0.78 & 0.68 & 0.38 \\
\hline
dsp(\neg Aut_X) & 0 & 0.03 & 0.03 & 0.16 \\
\hline
dsp(Trust_X) & 1 & 0.89 & 0.66 & 0.27 \\
\hline
dsp(\neg Trust_X) & 0 & 0.01 & 0.05 & 0.41 \\
\hline
\end{array}
\]
Implementation

(users a b c d)
(owner a)
(cert a b 0.9)
(cert a c 0.5)
(cert b c 0.6)
(a-rate c d 0.9)
(rev b d 0.3)
(t-rate b c 0.6)
(rec a b 0.8)
(rec a c 0.7)
(t-rate b d 0.7)
(show-args)
(show-dsp)

http://www.iam.unibe.ch/~run/trust.html
Outline

1. Introduction
2. Credential Networks
3. Evaluation
4. Conclusion
Conclusion

- Credential networks: new model for authenticity and trust evaluation
- A two-layer approach
- Allows gradual levels of trust and authenticity
- Evaluation is based on PAS
- A framework for specifying and evaluating credential networks has been implemented
  
  http://www.iam.unibe.ch/~run/trust.html
Thank you.
Any questions?