



# **A Service Provisioning System for Distributed Personalization with Private Data Protection**

---

**Hiroyuki KASAI**

**NTT DoCoMo, Inc. JAPAN  
Network Laboratories**

**28 June 2006**

# Service Scenario

Deliver tailored & personalized messages to users according to their private information.

*On a street...*

*I want to send a new CD album info. to people who like pop music.*



**Service Provider**



*At a shopping center entrance*

*I want to send an event news according to customer's profile.*



**User**

New Album  
"Moon"  
debut!



**User**

**Event news!**

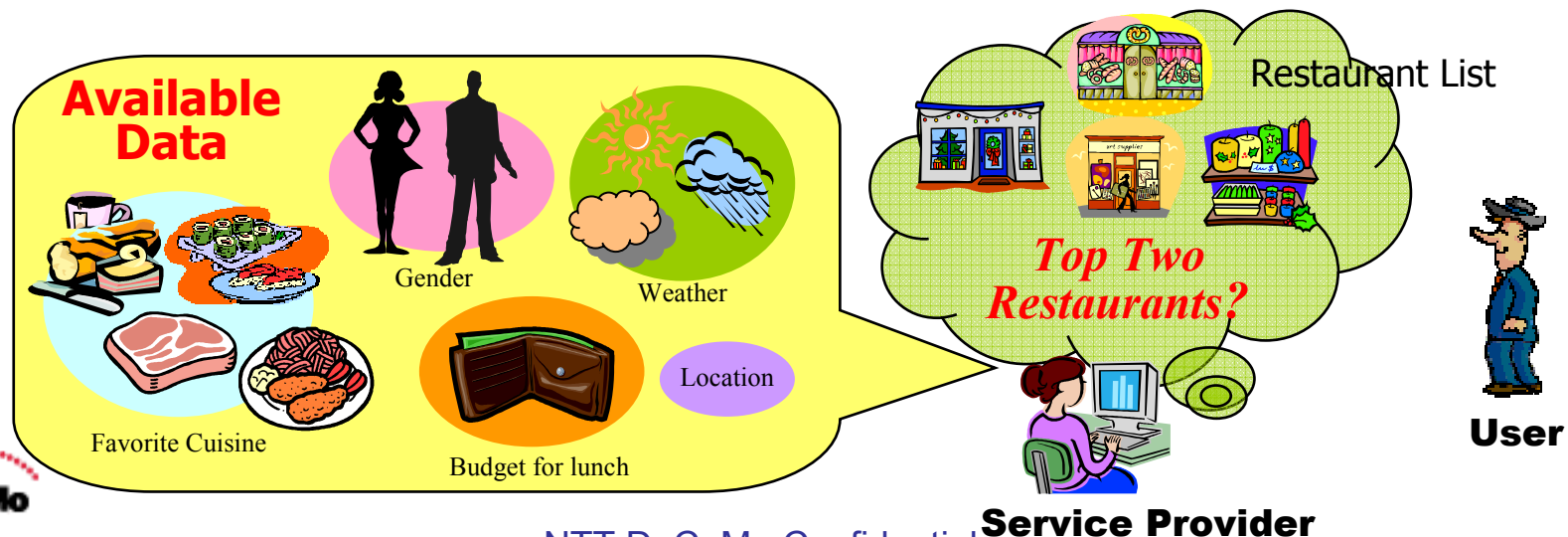
1. French restaurant is holding spring fair at (2F-E block).
2. How about Italian Gelato on this hot day?(1F-C block)
3. Fresh Japanese noodle ! (3F-A block)

# Service Rule for Customization

Adapt **service behaviors** (select, filter, sort, etc.) according to **various data** (user's profile/preference, location, weather, etc.).

## Service Rule

- Specifies service behavior and necessary data, and
- Tells effectiveness caused by messages.



# Issue in Ubiquitous & Open World

**Some data might be unobtainable.**

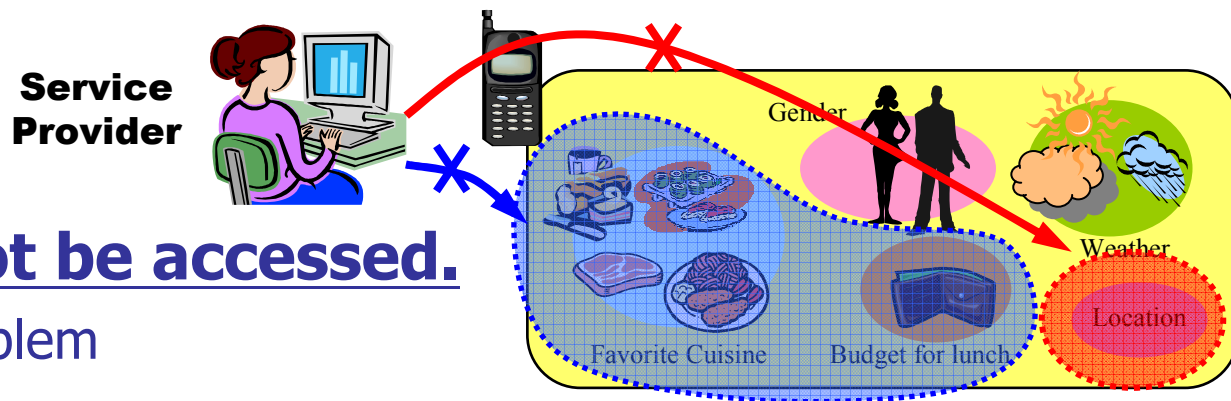
## 1. Data does not exist.

- A service rule might not operate properly.
- Missing data has an different influence on the service rule.

**Service assessment mechanism** that can judge how properly the service rule operates with missing data.

## 2. Data cannot be accessed.

- Privacy Problem



**Privacy preserving mechanism** which can provide a personalized service without revealing private data.



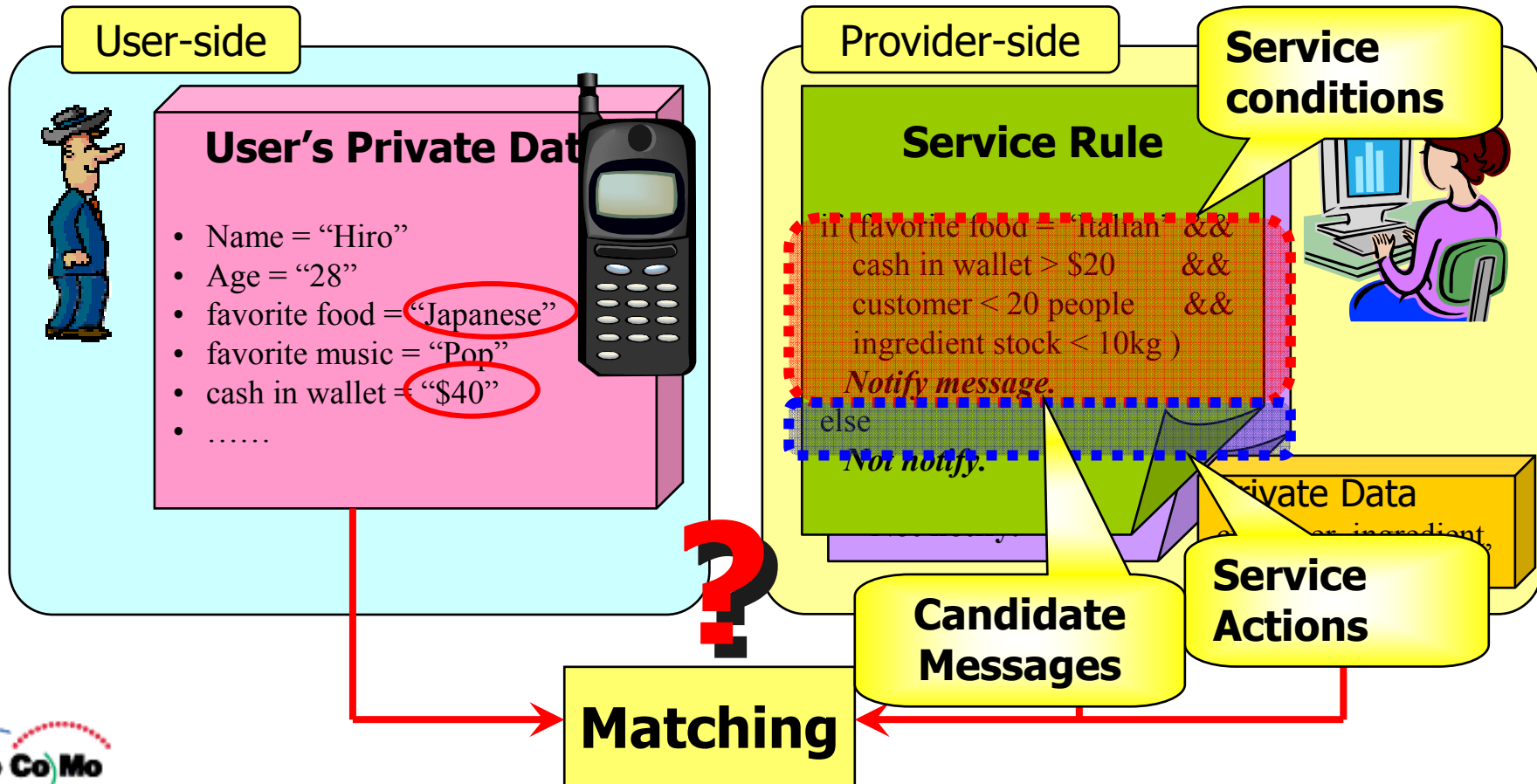
# Outline

## Privacy Preserving Service Execution Control based on Service Rule Sharing

1. Overview
2. Basic Mechanism
  - Service Rule Description based on BDN
3. Service Rule Conversion
  - Structure Conversion
  - CPT Conversion
4. Feature & Demonstration

# Assumption

Check whether **user's private data** meets a provider's "service rule."



# Problem & Motivation

- Problems for “User side”
  - **Trade-off** between available services and leak of private data.
  - **Big users’ burden** to determine appropriate disclosure policy at each situation.
- Problem for “Service provider side”
  - Leak of service rule, that is, their know-how.

Target!

Need service executable mechanism  
**without disclosing** user’s private data and  
provider’s service rules.

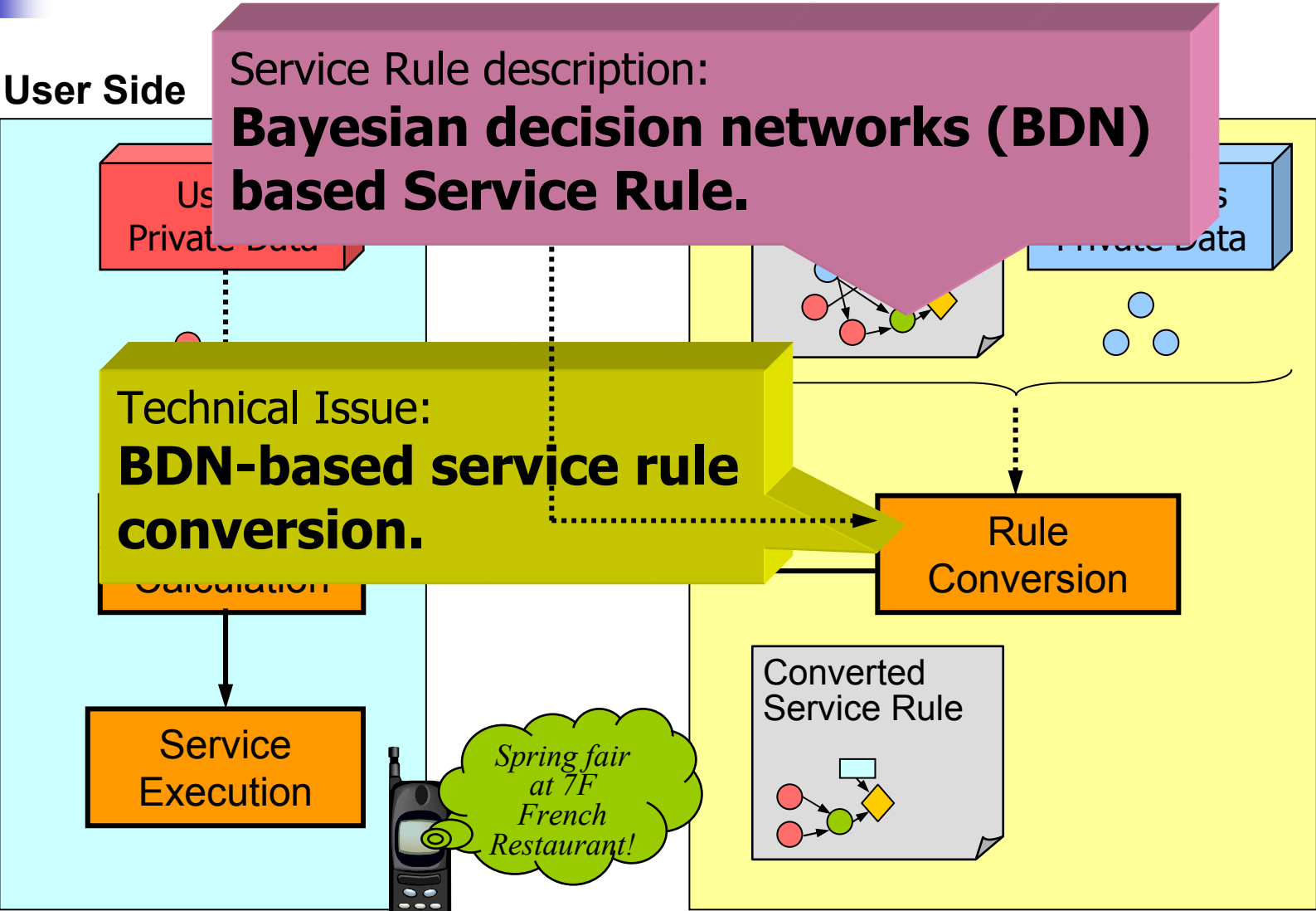
# Fundamental Policy & Proposal

- No reveal of user's private data:
  - Reveal **ONLY attribute data** of user's private data to *service providers*.
- No reveal of an entire service rule:
  - Reveal a **modified service rule** to *users*.

**Proposal!**

A service provider and a user **share** service execution procedure by exchanging a **converted (modified) service rule**.

# Basic Mechanism



# BDN-based Service Rule

## Bayesian Decision Network (BDN)

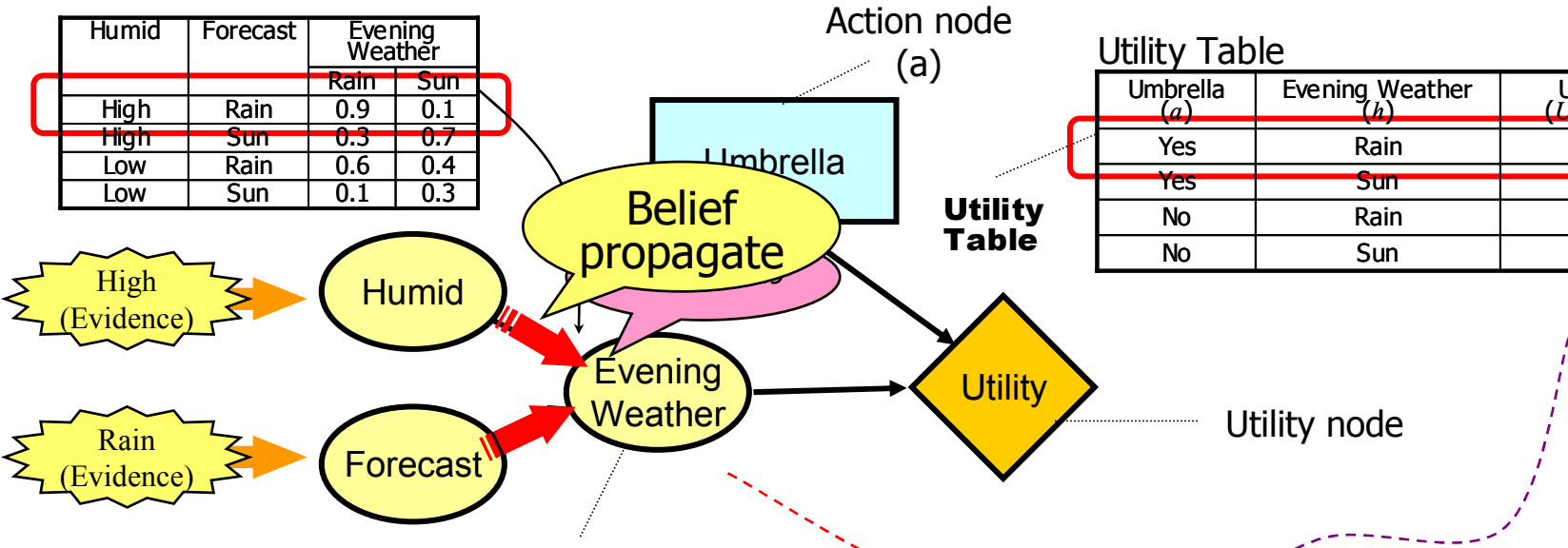
Bayesian network + Decision making NW

Conditional Probability Table (CPT)

Humid	Forecast	Evening Weather	
		Rain	Sun
High	Rain	0.9	0.1
High	Sun	0.3	0.7
Low	Rain	0.6	0.4
Low	Sun	0.1	0.3

Utility Table

Umbrella (a)	Evening Weather (h)	Utility (U(a,h))
Yes	Rain	9
Yes	Sun	2
No	Rain	3
No	Sun	-8



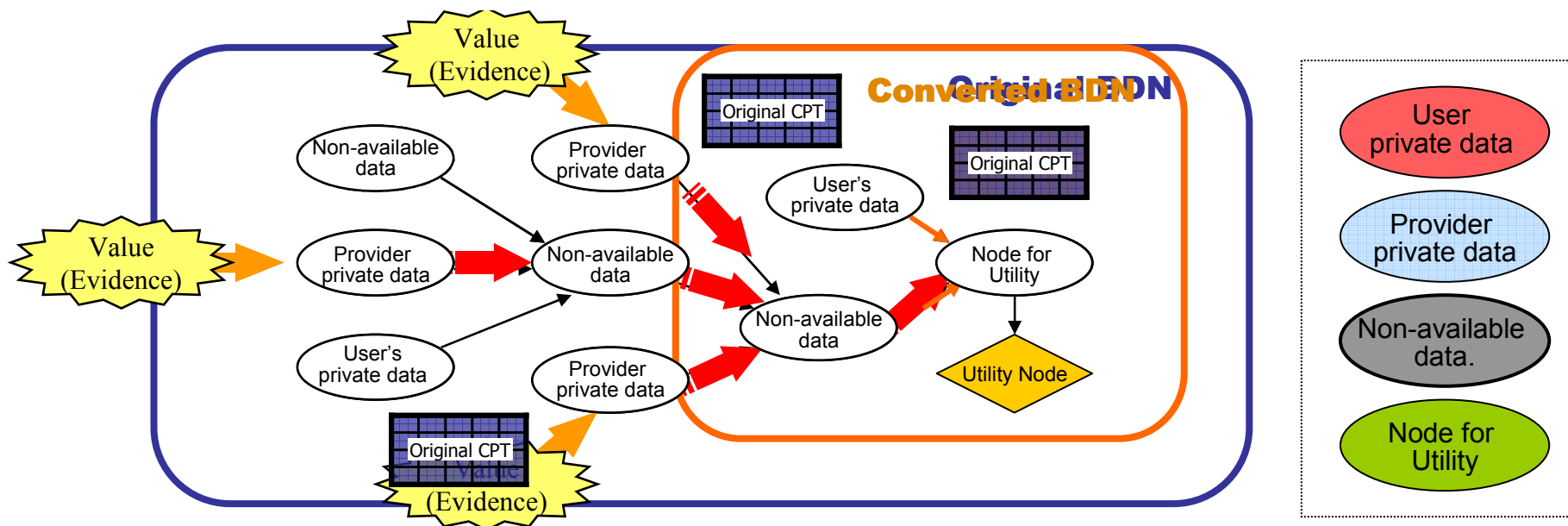
$$EU(a) = \sum_{h \in H} U(a, h) P(h)$$

$$opt(A) = arg \max_{h \in H} EU(a)$$

Select the action node with a MEU (maximum expected utility).

# Service Rule Conversion

Convert an original BDN into a new BDN with **ONLY** "user private data nodes" and "nodes for utility."

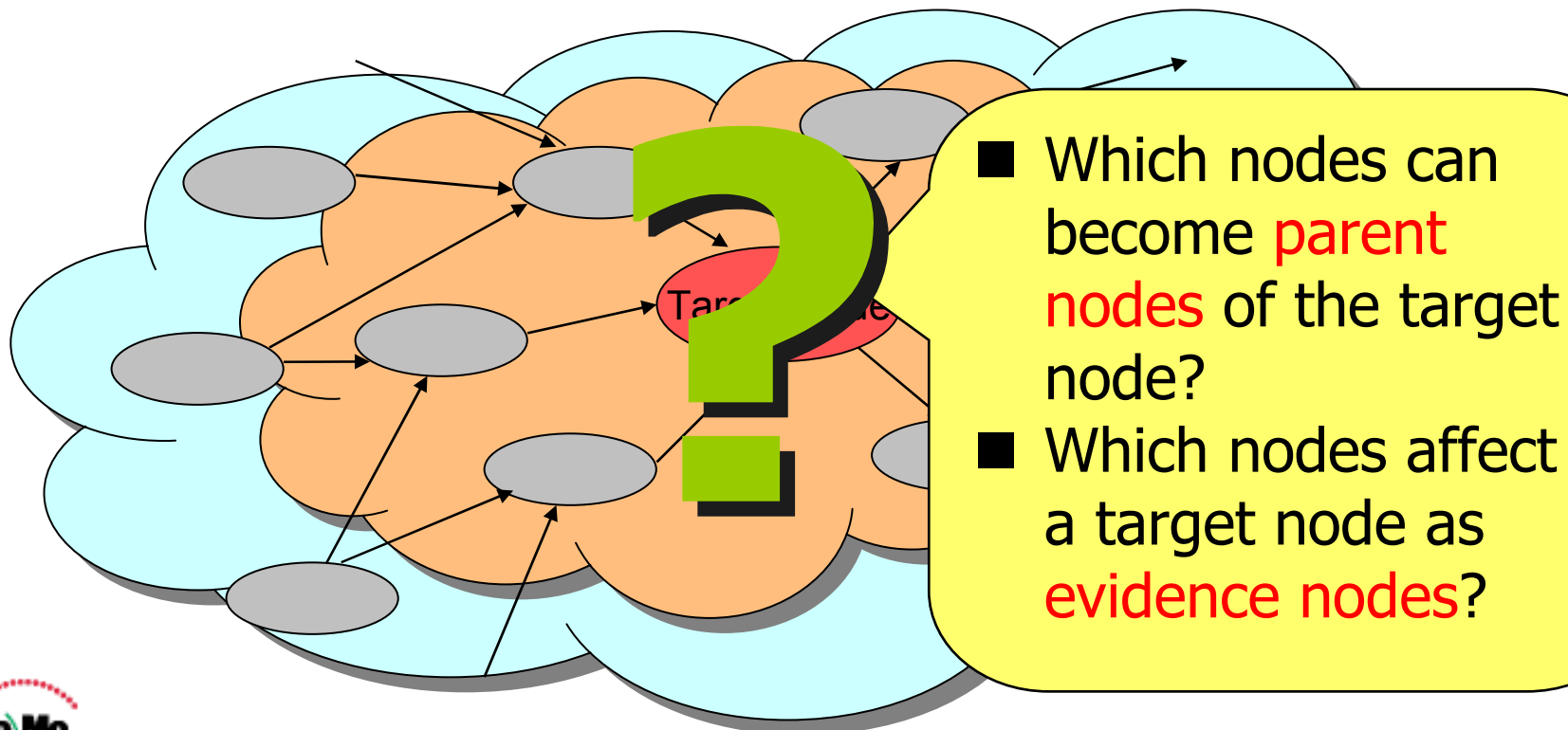


**Structure Conversion & CPT conversion.**



# Who are my parents?

Determine the nodes that have influence on **user private data nodes** and **nodes for utility** to be left.



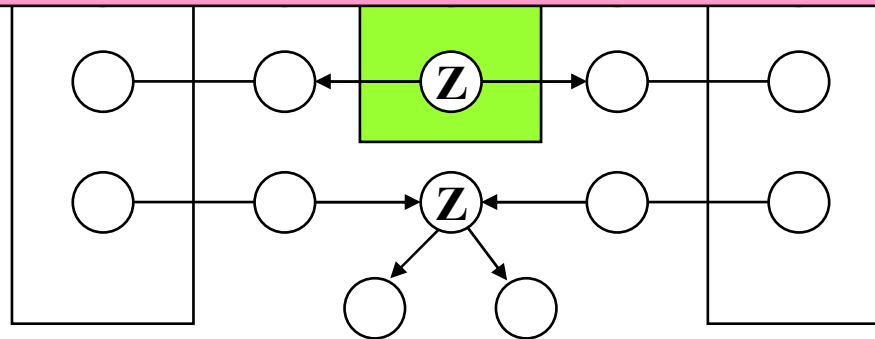
# Applying “d-separation”

**d-separation:** direction-dependent separation

*Point!*

If two nodes are “**D-separated**”, they

- are **conditional independent**, and
- have **no influence** on each other.



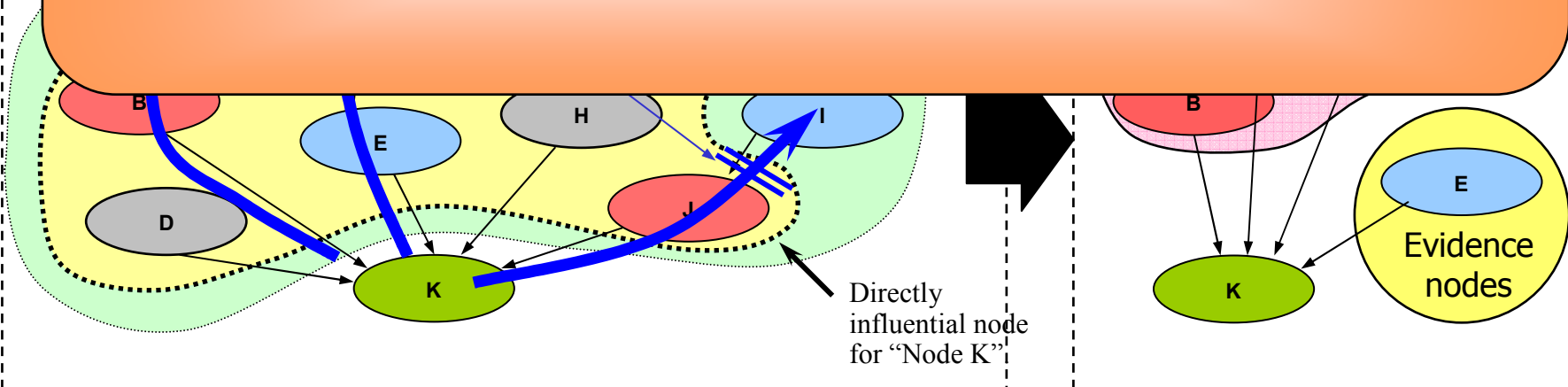
# Structure Conversion

**Determine influential nodes for remaining nodes.**

- List all nodes in upper stream of a remaining node.

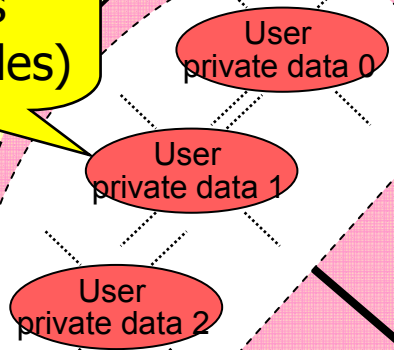
**Structure conversion has been completed !**

(Parent nodes and evidence nodes have been determined!)



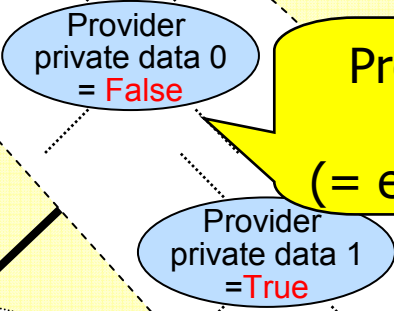
# CPT Conversion

User private data nodes (= parent nodes)



Directly influential node for a target node.

Provider private data nodes (= evidence nodes)



**Goal:**  
Calculate probabilities in all combinations of parent nodes.

**Execute Probabilistic Inference algorithm.**  
under  
**Parent nodes:**  
User private data 0 = True  
User private data 1 = True  
User private data 2 = False  
**Evidence nodes:**  
Provider private data 0 = False  
Provider private data 1 = True

No. (=l)	User Private Data 0	User Private Data 1	User Private Data 2	True	False
0	True	True	True	0.4	0.6
1	True	True	False	0.6	0.4
2	True	False	True	0.1	0.9
3	True	False	False	0.3	0.7
				0.5	0.5
7	False	True	True	0.8	0.2

parents  
states  
 $2^3 = 8$

# Features (Coverage)

## ➤ NOT suitable for

- Services that handle **a huge amount of information** (e.g. Conventional information search application from the whole of Internet.).

## ➤ Suitable for

- Service that select or sort information among **a limited number of candidate information** (e.g. location-aware pinpoint advertisement services, shop recommendation services).

# Advantages

➤ **More service opportunities:**

Users can receive and providers can give more services without disclosing their private data.

➤ **Mathematical Conversion:**

Conversion can be performed based on the mathematical calculation.

➤ **Strong protection of an entire service rule:**

One evidence input or one node elimination can propagate its influence on a large area inside NW.

➤ **Robustness for wrong user's declaration:**

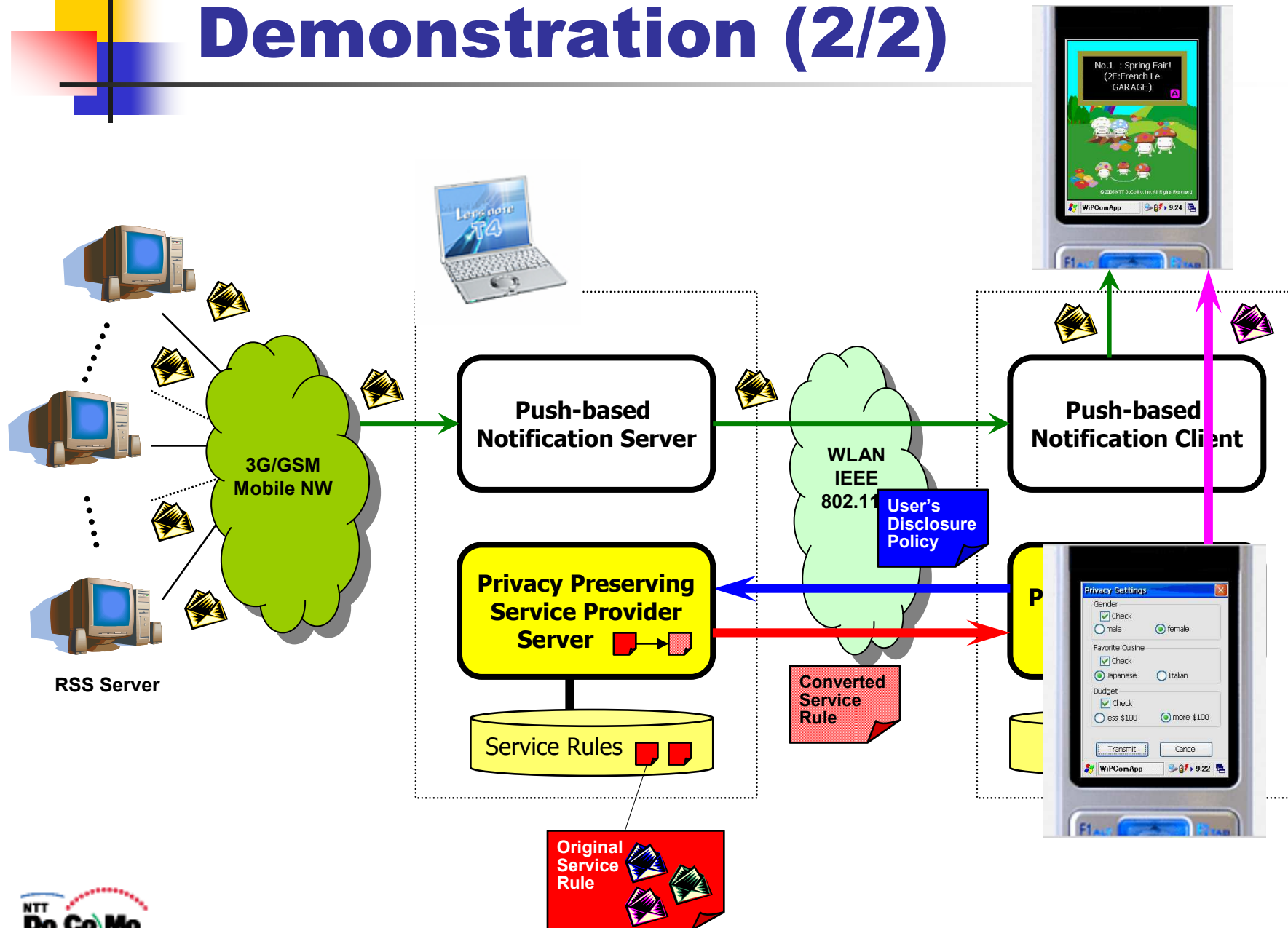
Even if some user's private data are missing when service execution at user-side, the converted rule can even work based on just available data.

# Demonstration (1/2)

## Demonstration Scenario

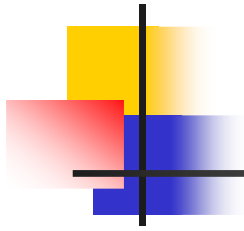
- A restaurant center sends select three best shops of five according to user's private data.
- User's private data are user's
  - budget for lunch,
  - favorite cuisine, and
  - gender.
- Prototype system is implemented on Push-based Notification System.

# Demonstration (2/2)



# Conclusions

- Propose a privacy preserving service provisioning mechanism by sharing service execution procedure in both user side and provider side.
- Achieve by exchanging converted service rules.
- BDN-based service rule description and service rule conversion algorithm.



**Thank you for your attention!**