



Australian Government

IP Australia

Discovery House, Phillip ACT 2606  
PO Box 200, Woden ACT 2606  
Australia  
Phone: 1300 651 010  
International Callers: +61-2 6283 2999  
Facsimile: +61-2 6283 7999  
Email: [assist@ipaaustralia.gov.au](mailto:assist@ipaaustralia.gov.au)  
Website: [www.ipaustralia.gov.au](http://www.ipaustralia.gov.au)

## Electronic Commerce Questionnaire

IP Australia is working to deliver consistency of service across all customer service channels. In order to achieve this consistency of service we must first clarify our E-commerce delivery rules and establish consistent standards. We are seeking your input into this process and would appreciate your feedback through the provision of answers to the following questions.

### Definitions

- **Authentication** - *Determining who exactly is performing a transaction: who's at the end of the line.*
- **Authorisation** - *Is the person performing the transaction allowed to perform the transaction, particularly when acting on behalf of a third party.*
- **PKI** – *A PKI (public key infrastructure) enables users of the Internet to securely and privately exchange data and financial details through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.*
- **Australian Government Authentication Framework (AGAF)** - *a whole-of-government approach to e-authentication. It recognises that different e-authentication mechanisms are needed for different types of transactions, depending on the degree of risk.*
- **Direct Debit** - *A pre-authorised debit on the payer's Australian bank account initiated by the recipient of the transaction (IP Australia).*

### Background

Electronic authentication (or e-authentication) is the process of establishing a level of confidence in whether a statement is genuine or valid. E-authentication is particularly important when transferring funds, disclosing sensitive information or making legally binding declarations. There are many approaches to e-authentication, ranging from usernames and passwords to digital certificates. Broadly speaking, e-authentication relies on one or more of the following:

- something that is known to both parties, such as a password or personal identification number (PIN), or
- other information known only to both parties (often referred to as 'shared secrets')
- identity checks such as the 100-point identity check,
- some form of identification that one party has, such as a digital certificate or PKI, or
- something that is a characteristic of a party, such as a fingerprint or iris scan.

The Australian Government e-Authentication Framework (AGAF) comprises a set of principles to guide government agencies in selecting appropriate e-authentication approaches. It is a transparent, risk management framework that will help businesses see how such decisions are reached.

### Credentials and protocols

The AGAF defines four levels of assurance for e-authentication – minimal, low, moderate and high. The determination of what assurance level to apply to a transaction or cluster of transactions depends on the residual risk associated with the transactions after taking into account the other forms of security and control in place around the transactions.

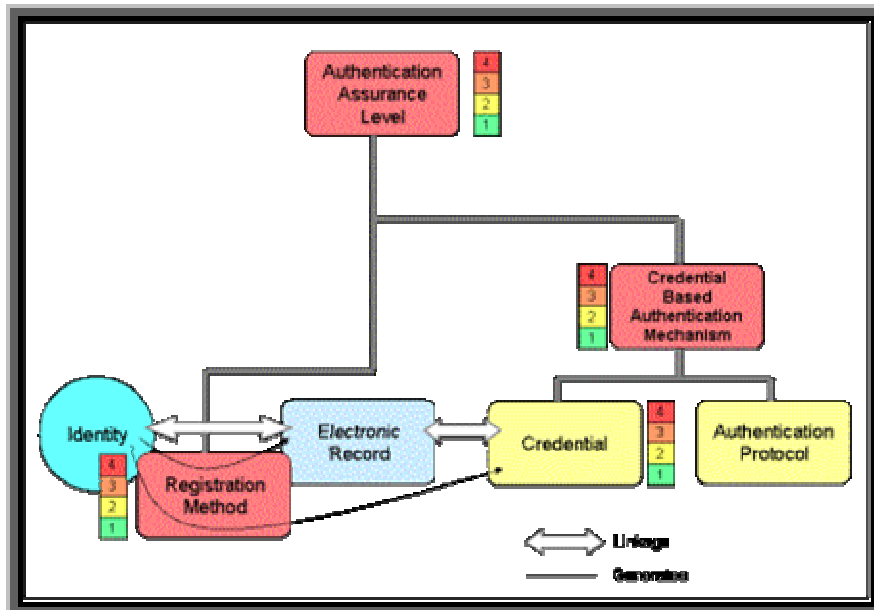
How the required assurance level is then met by an e-authentication approach is a function of the respective strengths of the credential used to verify the identity online and the underpinning registration method (that is, the process followed in issuing a user with a credential).

A credential may include a password, hardware token, smartcard or certificate. This is used in

conjunction with some e-authentication protocol. The e-authentication protocol addresses issues of exchange of information between the relying party and the user, protection of secret information by the user, relying party or trust-broker.

The term e-authentication mechanism is used to describe the amalgam of the credential and e-authentication protocol used to establish that a user is entitled to use a claimed identity.

The following figure shows the relationship between the solution components required to meet assurance levels.



**Figure 1.** Source: Australian Government e-Authentication Framework – better practice guide to authorisation and access management. ([http://www.agimo.gov.au/infrastructure/authentication/agaf\\_b/betterpracguide](http://www.agimo.gov.au/infrastructure/authentication/agaf_b/betterpracguide))

IP Australia recognises that different types of transactions need different e-authentication mechanisms, depending on the degree of risk involved. IP Australia intends to use the four assurance levels defined by AGAF depending on the degree of risk involved in the transaction (see Figure 2).

The AGAF assurance levels			
Level 1	Level 2	Level 3	Level 4
Minimal risk	Low risk	Moderate risk	High risk
Little requirement for e-authentication	Some requirement for e-authentication	Moderate requirement for e-authentication	High requirement for e-authentication

**Figure 2.** Source: Australian Government e-Authentication Framework ([http://www.agimo.gov.au/\\_\\_data/assets/pdf\\_file/40766/Low\\_res\\_Overview.pdf](http://www.agimo.gov.au/__data/assets/pdf_file/40766/Low_res_Overview.pdf))

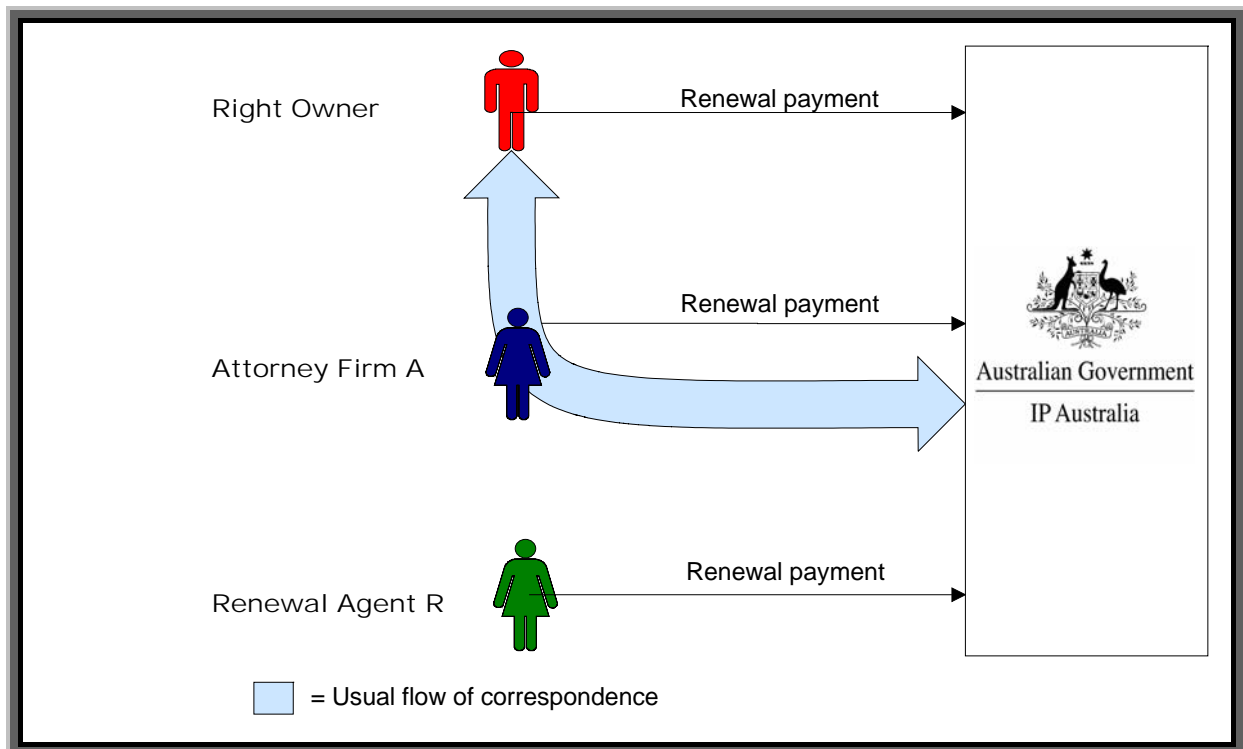
Subject to budgetary and policy constraints, IP Australia intends to meet AGAF requirements by:

- deciding what transactions needs to be authenticated – that is, what piece of information it is seeking to validate.
- deciding on the level of assurance needed – that is, how sure does the agency need to be that a statement is true, based on assessing the risks of getting it wrong
- selecting an appropriate e-authentication technique based on AGAF requirements – low-risk transactions require only a low-level e-authentication method such as username and password, while high-risk transactions require a high-level e-authentication method such as digital certificates, and
- confirming the proposed e-authentication approach by assessing various public policy principles, such as privacy and social equity and through stakeholder consultation.

## Scenario questions

The following scenarios are based on situations that currently occur in the administration of IP Rights as well as situations that are likely to occur in an e-commerce environment.

To assist IP Australia refine our e-authentication approach we ask that you look at the situations depicted in the scenario diagrams. We then ask that you provide answers to the questions below each scenario based on the different roles. We are interested in hearing your views from **all perspectives**.



### Scenario 1

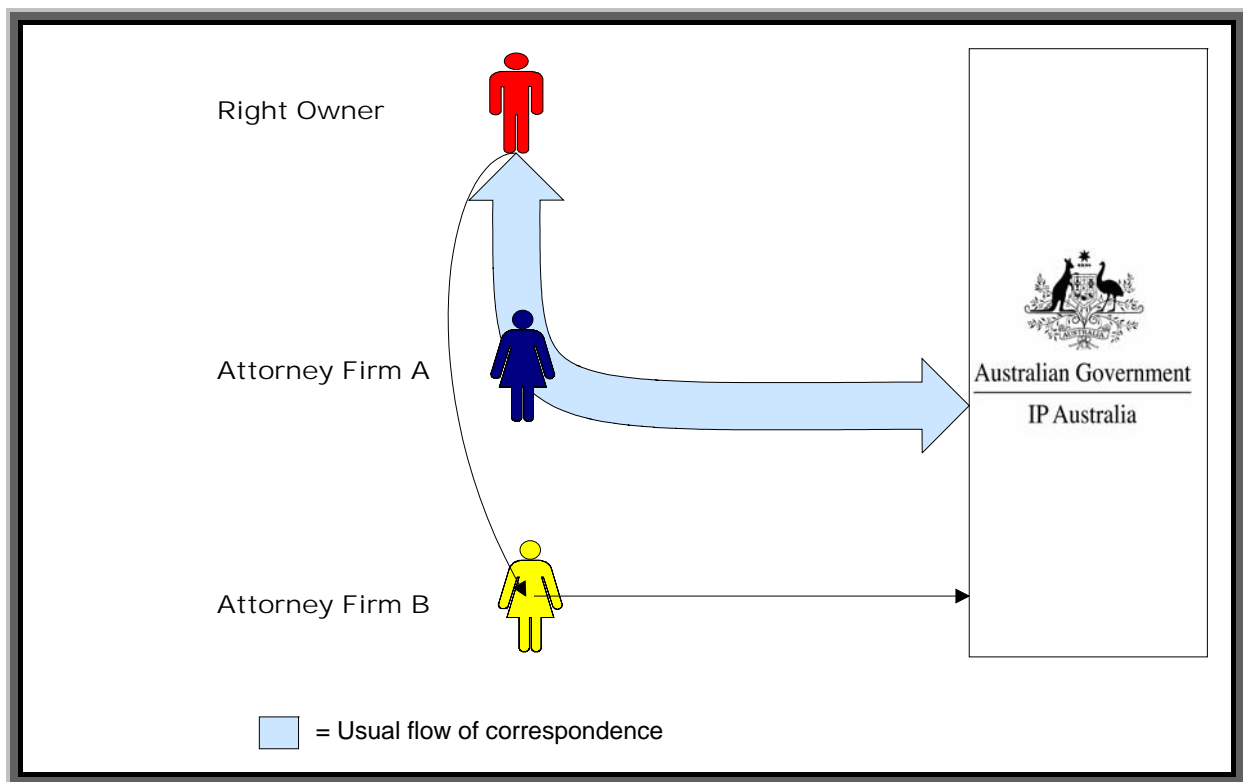
In scenario 1 IP Australia receives three separate renewal payments for the same renewal year on the one IP Right.

If you were the Right Owner in scenario 1,

- Which renewal payment would you want IP Australia to accept and process?
- Which parties would you want IP Australia to notify?
- If IP Australia experienced problems with the payment, such as insufficient funds, what action would you want IP Australia to take?
- If Attorney Firm A uses Renewal Agent R to manage your renewal payments. Who do you receive renewal payment notification from? What actions do you take when you receive this notification?

If you were the Attorney Firm A or Renewal Agent R in scenario 1,

- Which renewal payment would you want IP Australia to accept and process?
- Would you want IP Australia to accept the payment, even if the Address for Service (AFS) or PKI certificate does not match with any previous transactions on the IP Right?
- Which parties would you want IP Australia to notify?
- If your firm was **not** using Direct Debit as a payment method. What actions would you want IP Australia to take if problems were experienced with the payment, such as insufficient funds?
- If Attorney Firm A uses Renewal Agent R to manage renewal payments. Who notifies the Right Owner that a renewal payment has been made on their behalf?



### Scenario 2

In scenario 2 IP Australia receives a request for action against the IP Right from Attorney Firm B when all previous interactions have been with Attorney Firm A.

If you were the Right Owner in scenario 2,

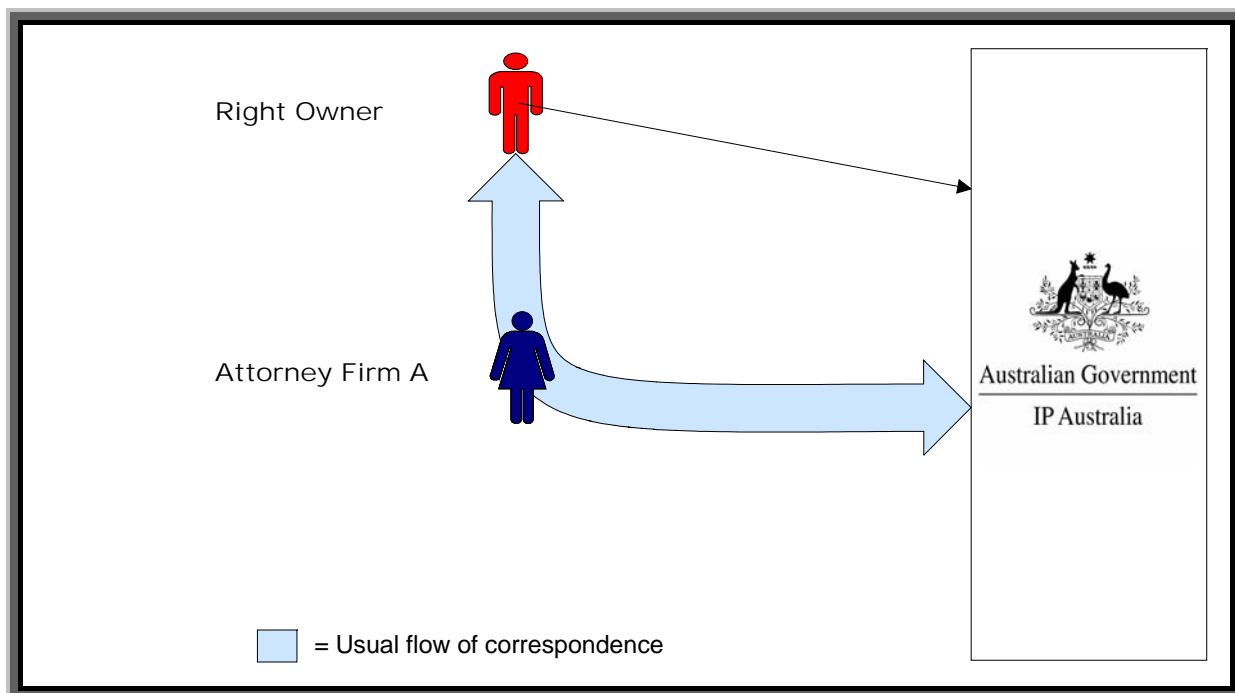
- Do you keep Attorney Firm A informed of any other actions?
- Would you inform IP Australia of the role and responsibilities of Attorney Firm B?
- Should IP Australia track credential changes? If so, do you have any comments on what level of detail IP Australia should record and how long IP Australia should retain these records for?
- In the absence of any instruction from the Right Owner or Attorney Firm A would you want IP Australia to act on the instruction, wait for instructions to be received or to seek clarification before acting? How long should IP Australia wait? Where would IP Australia seek clarification?

If you were Attorney Firm A in scenario 2,

- Do you receive notification from the Right Owner about the role and responsibilities of Attorney Firm B?
- Do you receive notification from Attorney Firm B about their role and responsibilities?
- If you receive notification from the Right Owner would you inform IP Australia?
- Should IP Australia track credential changes? If so, do you have any comments on what level of detail IP Australia should record and how long IP Australia should retain these records for?
- What actions would you want IP Australia to perform if the Right Owner informs IP Australia directly?
- What actions would you want IP Australia to perform if the Address for Service (AFS) or PKI certificate does not match with any previous transactions on the IP Right?
- In the absence of any instruction from the Right Owner or Attorney Firm A would you want IP Australia to act on the instruction, wait for instructions to be received or to seek clarification before acting? How long should IP Australia wait? Where would IP Australia seek clarification?
- In your experience, how often does this type of scenario arise?

If you were Attorney Firm B in scenario 2,

- Do you notify Attorney Firm A about the role and responsibilities assigned to you by the Right Owner?
- If you receive notification from the Right Owner would you inform IP Australia?
- Should IP Australia track credential changes? If so, do you have any comments on what level of detail IP Australia should record and how long IP Australia should retain these records for?



**Scenario 3**

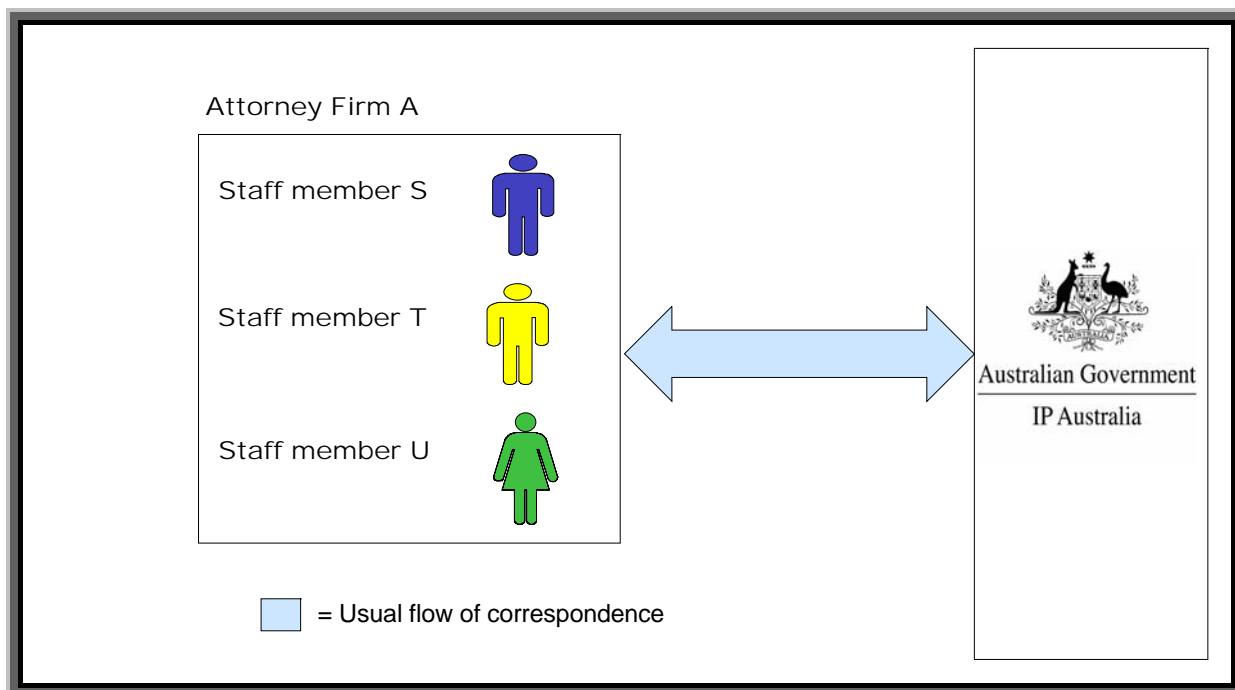
In scenario 3 IP Australia receives a request for action against the IP Right directly from the Right Owner .

If you were the Right Owner in scenario 3,

- Do you keep Attorney Firm A informed of these direct interactions with IP Australia?
- Who should IP Australia send notification to?

If you were Attorney Firm A in scenario 3,

- Do you receive notification from the Right Owner about direct interactions with IP Australia?
- If you receive notification from the Right Owner would you inform IP Australia?
- Would you want IP Australia to action requests or seek clarification if the Right Owner informs IP Australia directly and therefore the Address for Service (AFS) or PKI certificate does not match with any previous transactions on the IP Right?
- Who should IP Australia send notification to?

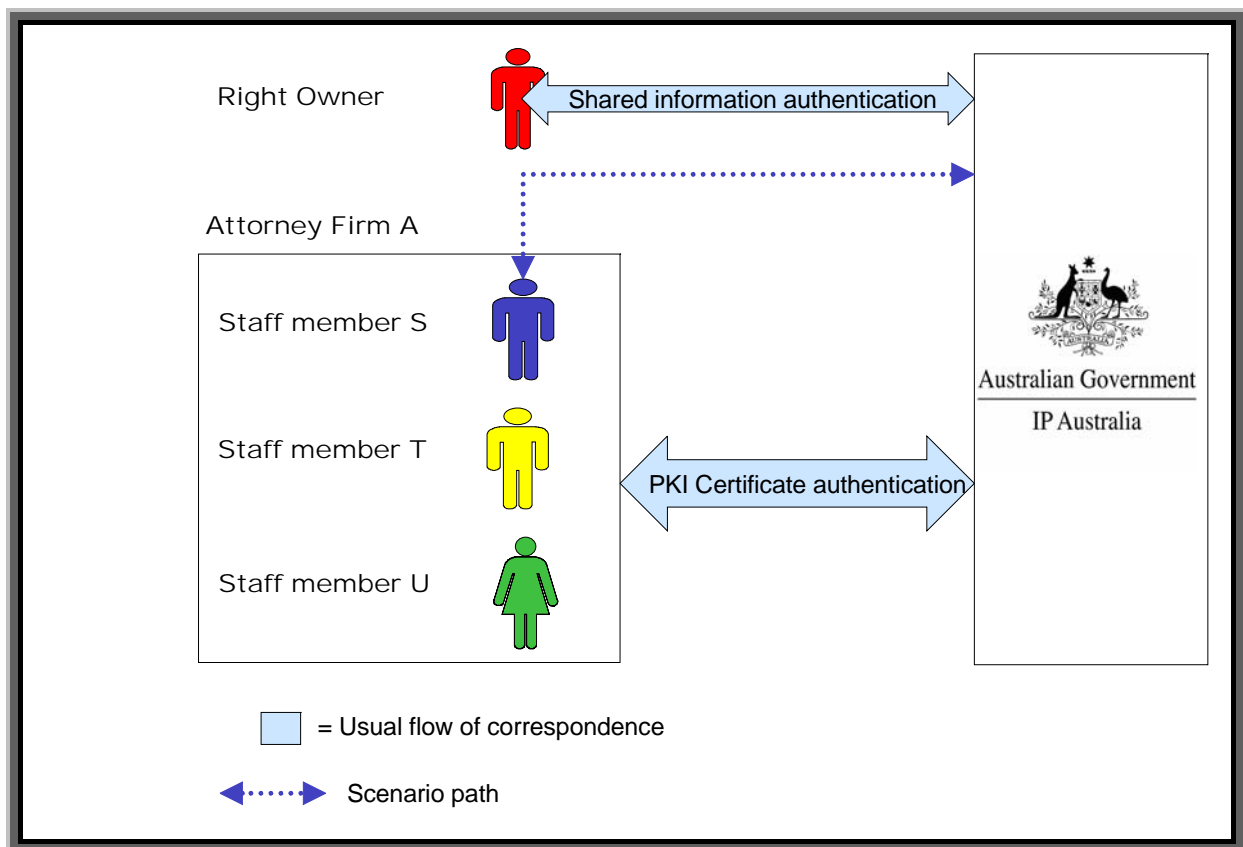


#### Scenario 4

In scenario 4 Attorney Firm A is using a single PKI certificate authentication when interacting with IP Australia. IP Australia will identify all the transactions in this scenario as coming from Attorney A. IP Australia will not be able to differentiate transactions received from staff member S, staff member T or staff member U.

If you were Attorney Firm A in scenario 4,

- Do you think that you have in place sufficient audit trails to trace individual transactions?
- When IP Australia sends back electronic correspondence and error messages relating to specific transactions how would you handle these? Would you have sufficient information to match the transaction with the initiating staff member?
- In order to assist you with your internal audit trails, would you like to see an optional field in transactions where you could place user ids or similar?
- Are there any other data fields you would want to pass to IP Australia in transactions?



### Scenario 5

In scenario 5 IP Australia may provide two alternative secure e-Commerce facilities.

1. *PKI certificate authentication* – Attorney Firm A is using a single PKI certificate authentication when interacting with IP Australia. IP Australia will identify all the transactions in this scenario as coming from Attorney Firm A. IP Australia will not be able to differentiate transactions received from staff member S, staff member T or staff member U.
2. *Shared information authentication* – The Right Owner is accessing IP Australia's online services using shared information authentication such as a userid, password and 'shared secrets' model.

If you were Attorney Firm A in scenario 5,

- Would you experience any problems if Staff member S decided to perform a new transaction, on behalf of Attorney Firm A, directly with IP Australia through the shared information authentication method (ie setting up his personal userid, password and shared secrets. Therefore Staff member S would have their own credentials via the shared information authentication as well as the firms PKI credentials.)? Is this a likely scenario?
- How would you track the flow of correspondence in this situation?
- What do you see as IP Australia's role in these situations?

What if Attorney A had previously been using username/password via the shared information authentication, then went to PKI: what would you like IP Australia to do with all the existing credentials?

## General questions

The experience of government in implementing online services has shown marked differences in the capacity of individuals and businesses to adopt particular e-authentication approaches. To enable IP Australia to identify potential impacts and implement a tailored approach could you please answer the following questions.

Would you identify yourself as?

- Individual IP Right owner
- Employee of a corporate IP Right owner
- Trade Marks Attorney
- Patent Attorney
- Designs Attorney
- Employee of Attorney firm
- Firm associated with IP Rights management. Please describe:.....

If you work in a firm, what size is the firm?

- Less than 5 employees
- Between 5 and 20 employees
- More than 20 employees

What is the physical location of your firm?

- Single location
- National distribution
- International distribution

What frequency of interaction would you or your firm have with IP Australia?

- Infrequent
- Daily
- Weekly
- Monthly

What government transactions do you or your firm currently complete online?

What levels of e-authentication currently occur in your firm? Do all staff have the same level of access to your internal electronic systems? Do you currently maintain audit records for access and permissions?

What level of PKI usage currently occurs in your firm? Does one PKI certificate service the whole firm? Are there different PKI certificates for each office? Are there different certificates for each PC and/or user?

Are there any other considerations you would like to add?

**Thank you for your participation!**